Design Models for Trusted Communications in Vehicle-to-Everything (V2X) Networks

Aljawharah M. Alnasser

A thesis presented for the degree of
Doctor of Philosophy at Durham University

Department of Computer Science
Durham University
United Kingdom

13th March 2020

Dedication

First, this thesis is dedicated to my beloved parents Mohammed and Albandari, whose love, help, support and prayers are the reason why I am where I am today. My dearest sisters Reem and Rehab who support me and make my life abroad much easier. My brothers Sami and Abdulrahman, who encourage me to complete my postgraduate study abroad. My beloved husband Abdulrahman, who makes my life full of motivations to achieve my goals, this thesis is for you.

Design Models for Trusted Communications in Vehicle-to-Everything (V2X) Networks

Aljawharah M. Alnasser

Submitted for the degree of Doctor of Philosophy
August 2019

Intelligent transportation system is one of the main systems which has been developed to achieve safe traffic and efficient transportation. It enables the road entities to establish connections with other road entities and infrastructure units using Vehicle-to-Everything (V2X) communications. To improve the driving experience, various applications are implemented to allow for road entities to share the information among each other. Then, based on the received information, the road entity can make its own decision regarding road safety and guide the driver. However, when these packets are dropped for any reason, it could lead to inaccurate decisions due to lack of enough information. Therefore, the packets should be sent through a trusted communication. The trusted communication includes a trusted link and trusted road entity. Before sending packets, the road entity should assess the link quality and choose the trusted link to ensure the packet delivery. Also, evaluating the neighboring node behavior is essential to obtain trusted communications because some misbehavior nodes may drop the received packets.

As a consequence, two main models are designed to achieve trusted V2X communications. First, a multi-metric Quality of Service (QoS)-balancing relay selection algorithm is proposed to elect the trusted link. Analytic Hierarchy Process (AHP) is applied to evaluate the link based on three metrics, which are channel capacity, link stability and end-to-end delay. Second, a recommendation-based trust model is designed for V2X communication to exclude misbehavior nodes. Based on a comparison between trust-based methods, weighted-sum is chosen in the

proposed model. The proposed methods ensure trusted communications by reducing the Packet Dropping Rate (PDR) and increasing the end-to-end delivery packet ratio. In addition, the proposed trust model achieves a very low False Negative Rate (FNR) in comparison with an existing model.

Declaration

Hereby declare that this thesis has been genuinely carried out by myself and has not been used in any previous application for a degree. Chapters 3 to 5 describe work performed by me with the guidance and support of my supervisors, Dr. Hongjian Sun and Prof. Gorden Love. These chapters have been published or submitted for publication (as shown in the publication list - Chapter 1).

Acknowledgements

All praise and thanks to Allah the All-Merciful the All-Beneficent, for granting me the ability and strength to complete this doctoral thesis. I am using this opportunity to express my gratitude to everyone who supported me throughout the course of this research. I am thankful for their invaluable guidance and friendly advice during the three years of this study. First of all, I would like to express my deepest appreciation to my supervisor Dr. Hongjian Sun who has supported me throughout my PhD study and provided me with supervision and guidance. I would like to express my appreciation to all the staff in the computer science department, technical support office and the library.

I am deeply indebted to my family, relatives and friends who offered me great encouragement and support throughout my studies. My heartfelt thanks go to my parents, my husband, my sisters and my brothers for their constant love, prayers, continuous support, and patience. Finally, I would like to gratefully acknowledge the provision of the scholarship from the Ministry of Higher Education in Saudi Arabia and the Saudi Cultural bureau in London.

Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1

Introduction

This chapter introduces the work conducted by this thesis in terms of explaining the motivation behind the research, aims and objectives. The chapter also explores the contributions made by the research work and lists the instances of previous publication of the results and outcomes. Furthermore, a brief description of the organization of the thesis is provided to explore the content of subsequent chapters.

1.1 Introduction

As a result of the massive spread of the Internet, a new notion has emerged which converts rigid objects to smart objects and connects them, known as the Internet of Things (IoT). IoT is achieved by embedding extra hardware such as sensors and communication interfaces within each device and linking them with a software system. Thus, the devices can sense the surrounding environment and share information using wireless communications. IoT has been broadly applied in various domains such as healthcare, smart cities and industry. Indeed, people spend the most times in homes, offices and transportation. According to the U.S. Department of Transportation

and Safety Administration, people spend 500 million hours per week in the vehicle [1]. In addition, based on Alcatel–Lucent's research, which was accomplished in 2009, they found that over 50% of participants liked the idea of connected vehicles and 22% are willing to pay fees for communication services [1] . Consequently, the need has been increased for joining the transportation system under the umbrella of IoT. Initially, the transportation system was transformed into a cyber-physical system by embedding software into vehicles. After that, vehicles have been developed to form a network and communicate with any smart device as a part of IoT. Generally speaking, the vehicular network is one of the main fields of network communications that has enormous number of entities to provide efficient transportation and safe driving experience.

Vehicle-to-Everything (V2X) technology supports intelligent transportation system where road entities, including vehicles, pedestrians, cycles, and motorcycles, and infrastructure units are interconnected with each other. This connectivity between them will produce more accurate information about the traffic situation across the entire network. Thus, it will help in improving traffic flows and reduce accidents. In 2015, Siemens implemented the first fully dynamic system on Germany's A9 highway. The result showed 35% fewer accidents and a reduction of people injured at roads with 31% [2].

Moreover, mobile nodes in vehicular networks cause an unstable and frequent change in the network topology, which leads to continuous change for the route between two nodes. Therefore, it results in short connection time between them and, in most cases, packets dropped due to link breakage. Thus, the packets should be delivered in a very short time, such as $100ms$ [3] for the guaranteed delivery. In addition, the existence of obstacles such as buildings and large trucks could affect the link quality. Indeed, some applications in vehicular networks such as safety-based application are delay-sensitive. Also, the packet dropping makes the decision on autonomous vehicles impossible, which causes a danger to the passengers. Therefore, evaluating the quality of available links before sending the packets is required to increase packet delivery rate, thus, improving the network performance.

Furthermore, the node behavior should be evaluated to ensure trusted communications. The existence of misbehaving nodes in the network could reduce the network performance by dropping

some or all of received packets [4]. The misbehaving nodes are authorized nodes that start behaving maliciously to disturb the network, which they are called internal attackers. The internal attackers are very hard to be detected as they look like normal nodes. Thus, a trust-based model is proposed to detect this type of attacks. Each node monitors its neighbors' behavior to detect any misbehaving nodes.

As a result, this thesis proposes novel computational models which achieve trusted communications in V2X network. The node and link trustworthiness are evaluated by considering security and Quality of Service (QoS) requirements in vehicular networks.

1.2 Statement of Aim

This thesis aims to design models that achieve trusted communications in V2X networks. The proposed models address some of the current research issues in the security and QoS requirements of heterogeneous vehicular networks.

1.3 Research Objectives

- **Objective 1:** To design a QoS relay selection algorithm for electing trusted links for communication in the V2X network.
- **Objective 2:** To design a recommendation-based distributed trust-based model for V2X networks that is ensuring communication with trusted nodes.
- **Objective 3:** To develop a hybrid trust-based model for V2X with global roaming capability that is able to protect the network against Road Side Unit (RSU) attacks.

1.4 Publications

The work in this thesis has been published and presented at several international conferences. A list of publications is provided based on the category of international conferences and journals as follows.

- **Journals**

  1. A. Alnasser and H. Sun, "A Fuzzy Logic Trust Model for Secure Routing in Smart Grid Networks," *IEEE Access*, vol. 5, pp. 17896–17903, 2017.
  2. A. Alnasser, H. Sun, and J. Jiang, "Cyber Security Challenges and Solutions for V2X Communications: A survey," *Computer Networks*, vol. 151, pp. 52–67, 2019. (Chapter 2)
  3. A. Alnasser, H. Sun and J. Jiang, "Recommendation-based Trust Model for Vehicle-to-Everything (V2X) Network", submitted to *IEEE Internet of Things Journal* - Minor revision.(Chapter 4)
  4. A. Alnasser, H. Sun and J. Jiang, "QoS-Balancing Algorithm for Optimal Relay Selection in Heterogeneous Vehicular Networks", submitted to *IEEE Transactions on Intelligent Transportation Systems.*(Chapter 3)

- **Conferences**

  1. A. Alnasser and H. Sun, "Performance analysis of behavior-based solutions in vehicular networks," in *Proc. of IEEE conference on Computer Communications Workshops (INFOCOM)*, 2018, pp. 736–741. (Chapter 4)
  2. A. Alnasser and H.Sun, "Global roaming trust-based model for V2X communications.," in *Proc. of IEEE conference on Computer Communications Workshops (INFOCOM)*, 2019. (Chapter 5)
  3. A. Alnasser, H. Sun and J. Jiang, "Multi-Metric QoS-balancing Relay Selection Algorithm in V2X Communications", Accepted for *IEEE Global Communication Conference (GLOBECOM).* (Chapter 3)
  4. A. Alnasser and H. Sun, "Trust-based model with protection against RSU attacks in vehicular networks", Accepted for *IEEE IPCCC.* (Chapter 5)

1.5 Research Contributions

The main contributions of this thesis are:

- A novel QoS-balancing relay selection model for V2X communication is proposed where the channel model for LTE-A (release 14) is applied for the first time.
- The outage probability is investigated for LTE-V2X communication protocol. The probability is examined for various parameters, which are distance, Signal-to-Noise Ratio (SNR) and SNR threshold. To the best of my knowledge, such a detailed study is not available anywhere in the literature.
- Based on the simulation results, Analytic Hierarchy Process (AHP) improves the decision making regarding the trusted link.
- A recommendation-based trust model for V2X communication is proposed. Different from existing research, it is a distributed model that detects non-stable behavior of internal attackers.
- Adaptive weights are applied in the recommendation filtering process. The weights are changed based on the number of positive and negative recommendations. Thus, the effect of the recommendation attacks is reduced.
- A global roaming trust-based model for V2X communications is proposed. Different from existing research, the nodes have global knowledge about untrusted nodes in the network.
- RSU attacks are studied for the first time. The proposed model can protect the network against them.

1.6 Overview of Thesis Structure

This thesis is structured as follows: first, this chapter (**Chapter 1**) introduces the work and explains the motivation behind it.

Chapter 2: Based on the published survey paper, the basic concept of V2X communication technology is introduced, exploring various security solutions that were proposed for detecting misbehaving nodes in vehicular networks. Also, various solutions for ensuring trusted communication links in the vehicular network are discussed. The open research issues for both categories

are presented.

Chapter 3: Based on the submitted journal and conference papers, a QoS-based relay selection algorithm for V2X communication is presented. The proposed algorithm applies the AHP-based algorithm to choose the most trusted link based on three main criteria, which are: channel capacity, link stability and end-to-end delay. Also, the outage probability for the V2X link is investigated.

Chapter 4: Based on the published journal and conference papers, a recommendation-based trust model for V2X communications is proposed. The novelty of this work is collecting recommendations and the computing of indirect trust. The proposed model is compared with an existing trust-based model to evaluate its performance. The results show that the proposed model outperforms the existing one. In addition, an analytical and simulation models of both models are proposed.

Chapter 5: Based on the published conference papers, the distributed decision system in Chapter 4 is improved and extended to be a hybrid decision system. It supports a distributed and centralized decision systems. For instance, the node is able to make its local decision in addition to the global decision. This type of schemes allows for global knowledge for all various entities regarding untrusted nodes in the V2X network. Thus, the proposed trust model supports global roaming security.

Chapter 6 presents a summary of the proposed research and summarizes the key findings. Also, it makes some recommendations for future work.

Chapter 2

Literature Review

This chapter provides a review of the literature to examine various security solutions for trusted communication in vehicular networks. It presents background information regarding V2X communication technology including architecture, communications and applications. Also, a threat analysis for various V2X communication protocols is discussed. In addition, various security solutions in vehicular networks are analyzed. Moreover, classification for the existing solutions, which achieve trusted communication links, is presented. Finally, it discusses the current challenges and research gaps in the vehicular network field.

2.1 Background of V2X Communication Technology

The intelligent transportation system applies data processing, communication, and sensor technologies to vehicles, infrastructure units, and roadside users to increase the safety and efficiency of the transportation system. The heterogeneous network consists of two main sub-networks [5] as shown in Figure 2.1:

- *Intra-vehicle network* comprises of a collection of sensors that are located in the vehicle. The interactions among sensors are bridged via Ethernet, ZigBee or WiFi connections.
- *Inter-vehicle network* covers the communication between the vehicle and surrounding devices. It comprises four entities as follows:
  - **On-board unit** is the primary entity in the intelligent transportation system. Each vehicle is equipped with an on-board unit to be able to process the collected data and interact with surrounding entities.
  - **Roadside users** such as pedestrian, motorcyclists, bikers and roller skates.
  - **RSU**is the transportation infrastructure unit that exists on the roadside. It has information about local topology that assists in providing several services to the road entities.

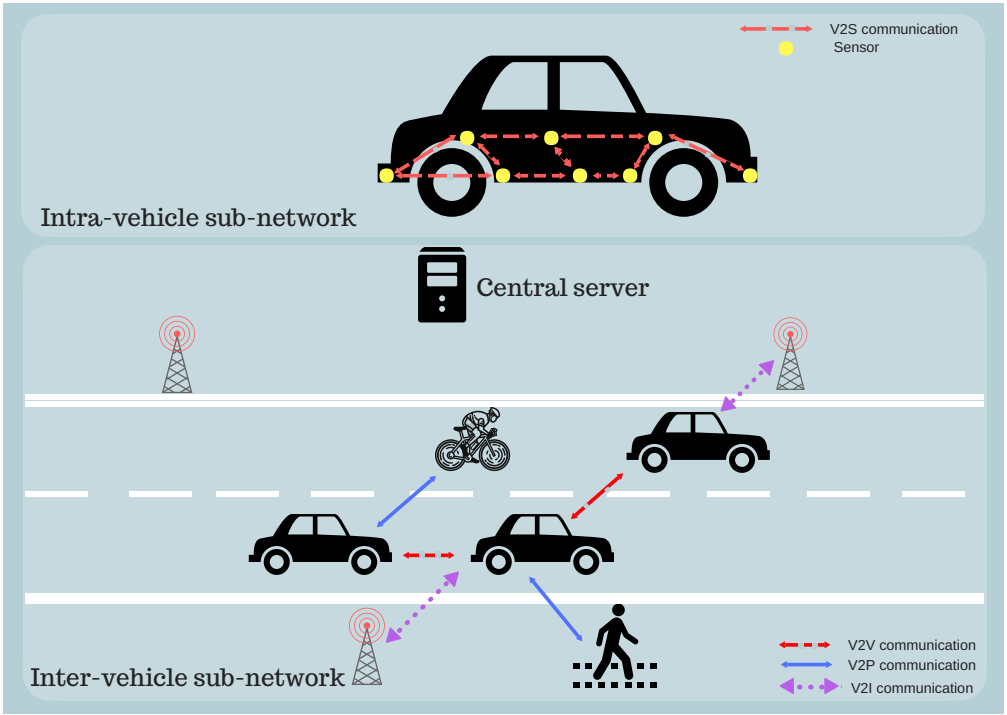


Figure 2.1: General structure of intelligent transportation system.

Table 2.1: V2X communication ranges

V2X connection link	Communication range
V2S	$10 - 100\ m$
V2V	$350\ m$ (for transmission power $=23\ dBm$) [7]
V2P	$170\ m$ (for lower transmission power $= 12\ dBm$) [7]
V2G	$350\ m$ (for transmission power $=23\ dBm$) [7]
V2I	$2000\ m$ [6]

– **Central/Cloud server** has a central control on all road entities, traffic and roads.

V2X has a unified connectivity platform for the connected entities. Also, it allows road entities to share information with their fixed and moving neighboring entities. The communication type depends on the entities that establish the link. V2X supports five types of communications [6] with various communication ranges, as shown in Table 2.1:

- *Vehicle-to-Sensors (V2S)* represents the communication between sensors in intra-vehicle sub-network;
- *Vehicle-to-Vehicle (V2V)* covers the communication between vehicles using V2V application;
- *Vehicle-to-Pedestrian (V2P)* provides the connection between the vehicle and roadside users;
- *Vehicle-to-Grid (V2G)* supports the communication between vehicles and the electric grid to charge electric vehicles;
- *Vehicle-to-Infrastructure (V2I)* represents the communication between road entities and infrastructure units.

In a vehicular network, all road entities are supposed to generate and exchange messages. The messages can be used to support a variety of applications, e.g., applications related to safety, traffic and infotainment. The messages are categorized into four types [3]:

- **Periodic message (beacon):** Road entities periodically broadcast a status message, which contains information about their current status such as speed, location and direction, to the neighboring entities. It is generated at regular intervals between $100ms$ to $1s$. As a result, each entity can perceive the local topology. Also, it can predict and anticipate dangerous situations or traffic congestion. This type of messages is not time critical.

- **Unicast message:** The road entity sends unicast messages to the core network for Internet services. Some of these messages contain confidential information such as credit card number.

- **Local event triggered message:** The road entity sends the message when a local event is detected such as the critical warning or intersection assist. It is sent locally to the neighboring entities using V2V/V2P links where it contains useful information for neighborhood area only. In addition, it is a time critical which requires to be delivered with a low latency around $100ms$.

- **Global event triggered message:** The road entity sends the message when a global event is detected such as road construction and road congestion. This message needs to be propagated over a wider area. As a result, road entities use V2I communication link to transmit the message.

- **Emergency vehicle message:** It is used to support a smooth movement for emergency vehicles. It is sent by emergency vehicles to the surrounding vehicles using V2V/V2P links to clear the road.

As a result of the technological improvements in the areas of sensing and wireless networking, intelligent transportation system permits for the existing of various applications that are related to safety, traffic, and infotainment [5]:

- *Safety-related applications* use wireless communications between surrounding entities to decrease accidents and protect the commuters from dangers. Each road entity periodically

sends safety messages to its neighbors to report its current status. Furthermore, they may also need to transmit warning messages when a local or global event is detected.

- *Traffic-related applications* are deployed to manage the traffic efficiently and ensure smooth traffic flow. They are responsible for collecting the traffic information and transmitting them wirelessly to a remote server for analysis. After that, the analysis results are sent to road entities for future usage.

- *Infotainment-related applications* aim at improving the driving experience by supporting various services such as Internet access, online gaming, video streaming, and weather information.

2.2 Security Service in V2X Technology for Trusted Communications

2.2.1 Security for Various V2X Enabling Technologies

Supporting safety-related applications is the core of vehicle-to-vehicle communication. Since ten years ago, V2X technology has been enabled by IEEE802.11p, which has been standardized, implemented, and examined.

One of the most critical challenges to make V2X technology feasible is how to ensure interoperability among heterogeneous devices. As a result, the 3^{rd} Generation Partnership Project (3GPP) has worked on standardization for the Long-Term Evolution (LTE) protocol to fit the requirements and services of the V2X communications. 3GPP has concentrated on supporting different types of communications using one standard. The first release (Release 8) was in 2008. The standardization of LTE Advanced Pro (Release 14) was finalized at the beginning of 2017 [6], which is called LTE-V2X. The safety of commuters relies on the performance of these technologies. Consequently, it is crucial to analyze the security services offered by these technologies.

Security Measures for V2X Communication Protocols

IEEE802.11p

It is an enhanced version of the ad-hoc mode in IEEE802.11a. It was implemented for supporting the communication between mobile nodes with the presence of obstacles, dynamic topology and intermittent connection. The main purpose of IEEE802.11p is to support non-line of sight [8]. It was proposed for supporting intelligent transportation system applications in Vehicular Ad-hoc NETwork (VANET). It provides ad-hoc communication between vehicles and RSUs. It gives vehicles the ability to share information with their neighboring vehicles and RSU using V2V and V2I only. IEEE 802.11p can be easily deployed with minimum cost, however, it lacks of scalability, limited delays, and QoS. Furthermore, it can only offer intermittent V2I connectivity because of the short radio range [9].

IEEE P1609.2 is based on cryptography standards such as elliptic curve cryptography, wireless access in vehicular environment certificate formats, and hybrid encryption methods [10]. *Broadcast Messages* are usually not directed to particular destination and they are related to safety-related applications. Also, they contain the timestamp which is obtained from the internal clock for synchronization. However, these messages are only signed with the sender's certificate. Elliptic Curve Digital Signature Algorithm is the signature algorithm that is applied this standard [11]. *Transaction Messages* are generally unicast messages and they may be used to access location-based services and personal data. Consequently, to protect the data, these messages are encrypted with a symmetric encryption algorithm. To ensure more protection, the algorithm uses a random key which is encrypted using elliptic curve integrated encryption scheme [11].

LTE-V2X

It has the potential to deal with the low-latency and high-reliability V2X use cases. LTE-V2X is mainly composed of six main components [6] as shown in Figure 2.2:

- *User Equipment (UE)* is the device that is used directly by the end-user to communicate with Evolved Node B (eNB) or other UEs.

- *eNB* is the wireless interface for LTE network which allows for sending and receiving radio transmissions to/from all UEs in one or more cells.
- *V2X Application Server* is responsible for distribution of V2X messages to different target areas.
- *V2X Control Function* is responsible for authorization and revocation of V2X services. It provides various services after successful mutual authentication and security key generation.
- *Multimedia Broadcast Multicast Service* supports efficient delivery for multicast services over areas typically spanning multiple cells.
- *Single-cell Point-to-Multipoint* provides the delivery of multicast services over a single cell.

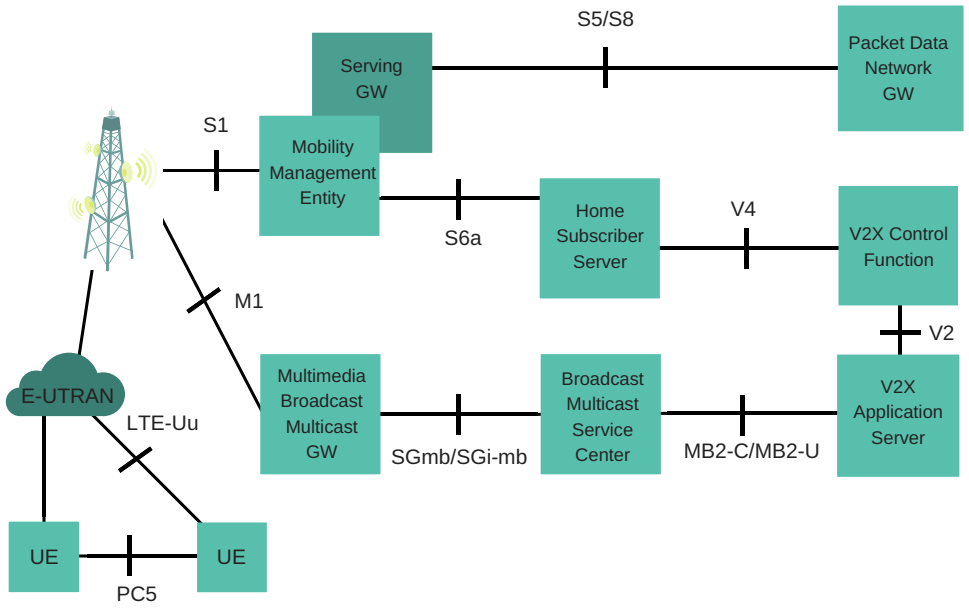


Figure 2.2: General structure of LTE-based V2X network.

In addition, a description for the reference points in Figure 2.2 is presented as follows [6]:

- **SGmb/SGi-mb/M1/M3:** reference points are internal to the MBMS system.
- **S1:** In case of V2X Service it is also used to convey the V2X Service authorization from MME to eNodeB.
- **S6a:** In case of V2X Service S6a is used to download V2X Service related subscription information to MME during E-UTRAN attach procedure or to inform MME subscription information in the HSS has changed.
- **V2:** The reference point between the V2X Application Server and the V2X Control Function in the operator's network. The V2X Application Server may connect to V2X Control Functions belonging to multiple PLMNs.
- **V4:** The reference point between the HSS and the V2X Control Function in the operator's network.
- **MB2-C/MB2/U:**The reference point between the V2X Application Server and the BM-SC.

In LTE-V2X, the messages are sent using two types of links, as shown in Figure 2.3:

- *Cellular-based communication* covers the two way communication between UE and eNB over LTE air interface [12]. The communication going from UE to eNB is called uplink and when it is going from eNB to a UE it is called downlink. Cellular-based communication covers wide area with high capacity. It is used by V2X application server to broadcast messages to vehicles and beyond, or send them to the UE via a unicast connection. In addition to one-to-one communications between eNB and UE, eNB supports one-to-many communications via downlink. eNB uses single-cell point-to-multipoint service for the transmissions over a single cell and multimedia broadcast multicast service for communications over multiple cells.

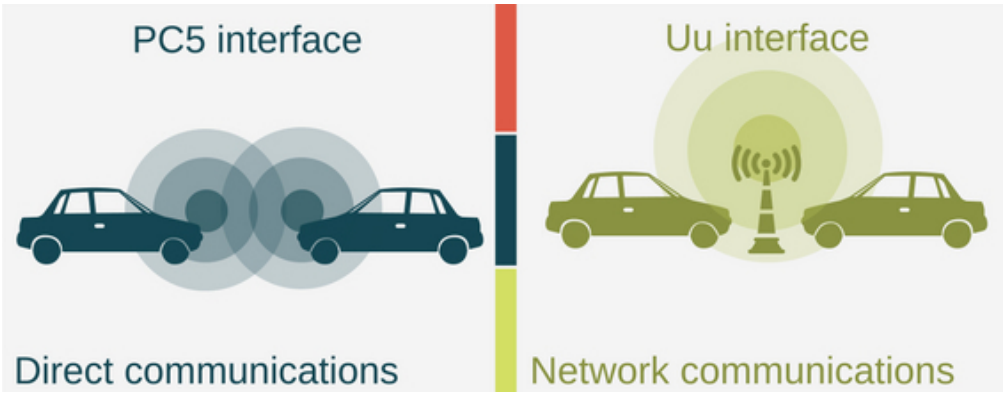


Figure 2.3: Communication links in LTE-V2X

- *Device-to-Device (D2D) communication* enables the direct connection between UEs without traversing eNB and it is called side-link. It supports multi-hop communications between network entities to enhance the end-to-end connectivity. Also, it provides a short-range communication and low latency for safety messages. As the most safety messages are critical and need to be delivered to the surrounding nodes in a very short time, sending them using D2D to the neighboring entities is faster than sending them through the cellular link to the core network to forward them to the entities which connected to the network. It allows for UE to transmit data directly to other UEs over the sidelink even if they reside out-of-network coverage. D2D link is used in three scenarios as shown in Figure 2.4 [13]. First, *in-network coverage scenario* where D2D communication is established between two UEs that are located in-network coverage. It is managed by eNB for load balancing or content sharing. Second, *relay coverage scenario* where D2D communication is established between UEs, when one of them is located out of the network coverage, to deliver the packets to eNB. The relaying nodes act as a range extender of the cell. Third, *out-of-network coverage scenario* where D2D communication is established by UEs which are located out of the network coverage. It is used for event messages, periodic messages and sharing content. Moreover, every D2D pair can communicate via *Inband* or *Outband* modes [12]. **Inband mode** uses the cellular spectrum for both D2D and cellular communications. *Underlay communication* allows for both of them sharing and reusing the same radio

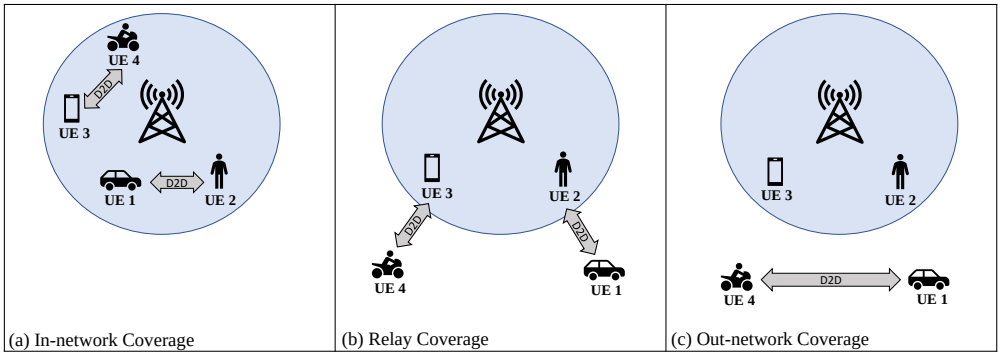


Figure 2.4: D2D communication scenarios

resources to improve the spectrum efficiency. The main drawback is the high possibility of collision between D2D links and cellular links. In contrast, *overlay communication* allocates dedicated cellular resources for D2D connections between the transmitter and the receiver. To minimize the interference between D2D and cellular links, **outband mode** uses unlicensed spectrum such as 2.4 GHz industrial, scientific and medical radio band. However, it is necessary to have an extra interface that implements Wi-Fi Direct or Bluetooth.

In D2D communication, the UE send the message to the neighboring UEs through PC5 reference point. PC5 is the reference point between the UEs used for user plane for ProSe Direct Communication for V2X Service [6]. On the other hand, when the V2X application in the UE would like to deliver the message over multiple cells, the message is sent through LTE-Uu reference point to the eNB. Then, the multimedia broadcast multicast service allows for broadcast message over multiple cells. The V2X application server is responsible for delivering data to the UE(s) in a target area using Unicast Delivery and/or MBMS Delivery [6]. There is a communication between V2X application server and V2X Control Function through V2 reference point. V2X Control Function is used to provision the UE with necessary parameters in order to use V2X communication. It is used to provision the UEs with PLMN specific parameters that allow the UE to use V2X in this specific PLMN. V2X Control Function is also used to provision the UE with parameters that are needed when the UE is "not served by EUTRAN" [6].

In LTE-V2X, RSU can be implemented in two ways [6]. *First*, it can be executed as stationary UE; then it receives V2X messages via the sidelink as shown in Figure 2.5 (a). In this case, the V2X application can communicate with other V2X applications. *Second*, it can be implemented in eNB, where it receives V2X messages via LTE radio interface as shown in Figure 2.5 (b). In this case, V2X application in UE communicates with the V2X application server in eNB.

There are two types of LTE security mechanisms based on the type of communications as follows.

- *Cellular-based communications:* There is a mutual authentication between UE and the core network. This is achieved by using the evolved packet core authentication and key agreement procedure and generating ciphering key and an integrity key. Moreover, UEs apply different keys for different communication sessions where session keys are produced

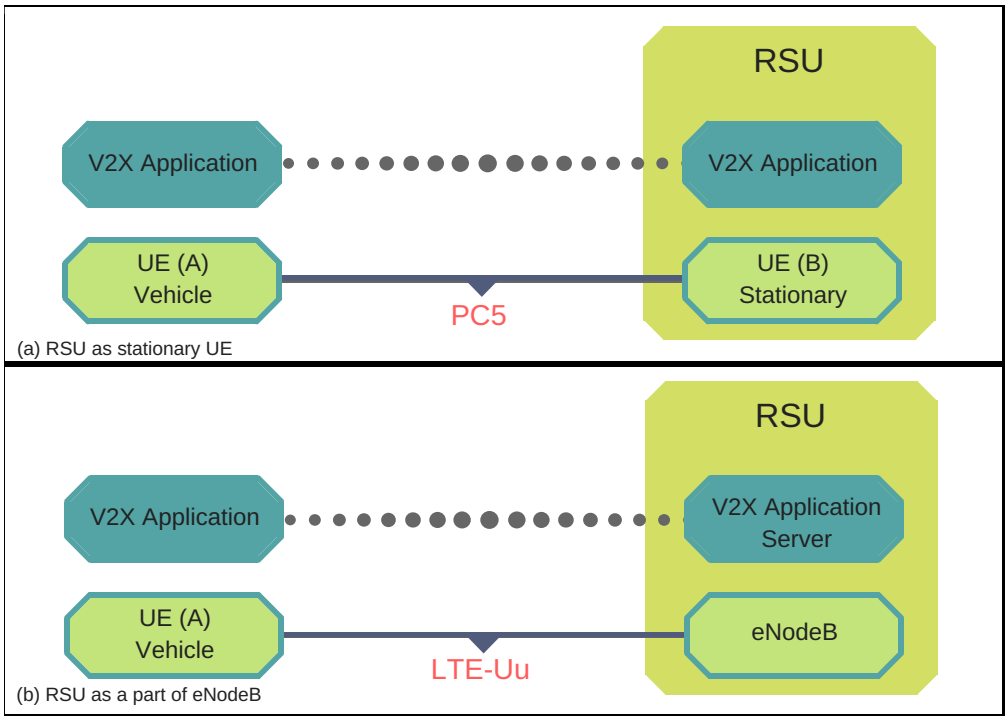


Figure 2.5: RSU implementation in V2X networks

using ciphering key and integrity key [7]. When an UE connects to the LTE network over the LTE radio interface, the mobility management entity is responsible for executing a mutual authentication with the UE. *First*, the UEs send authentication requests to the mobility management entity. *Second*, the mobility management entity checks the request validity and forwards it to home subscriber server, which is combined with the authentication centre, to manage and check user authenticity. *Third*, the authentication center generates and sends the authentication vector for specific UE to the mobility management entity [14]. However, the token that is sent by UE is not encrypted and is not integrity protected. After mutual authenticated, the key is exchanged between the mobility management entity and UEs, then the UEs will be able to access the core network. UE uses a pre-shared symmetric keying and integrity algorithm for signalling packets that is sent to the network. However, for user plane data, only ciphering algorithm is applied between UE and eNB [15].

- *D2D communications:* Before starting D2D communication, UEs have to finish authentication procedure with the core network [16]. Because the core network is responsible for managing the security parameters, the availability of accessing the network will directly affect the security level of D2D communications. The secure connectivity of UEs is based on three scenarios [17]. *In-network coverage* both UEs can communicate securely by the assist of the core network; *relay coverage* where the communication is also managed by the core network, thus, both UEs can establish a secure communication; and *out-network coverage* where each UE saves the authentication vector which is released by the authentication center for securing D2D communications [16]. The authentication parameters are valid for specific time and they might be revoked at any time, however, the security risk is increased.

  To overcome this challenge, each group has a group ID, which is corresponding to the Proximity Services (ProSe) group ID (layer 2), Algorithm ID and ProSe group key. Also, each UE within the group has a particular member ID [7]. Each ProSe group key is provided with an expiry time. When the UE is located out-of-network coverage, it may work for a longer time without extra provisioning when ProSe group keys valid at that time. The data in D2D communication is encrypted by ProSe encryption key which is derived from ProSe group key [7]. In this case, the confidentiality requirement is achieved

in data transmission. However, there is no integrity protection on the user data because the integrity key is shared by all group members.

Threats Analysis for V2X Communication Protocols

Similar to most communication networks, V2X security requirements can be divided into five points: availability, integrity, confidentiality, authenticity and non-repudiation [18]. However, in the V2X environment, attacks which targeting information availability and integrity are the most dangerous because they cause a serious effect on safety-critical situations. The following presents the security requirements for V2X network and threats against each one. Also, the security analysis for IEEE802.11p and LTE-V2X is considered.

Threats on Availability

They prevent the authorized users from accessing the information such as:

- *Blackhole and Greyhole attacks:* the compromised node stops relaying packets to the neighboring nodes. Thus, it blocks up the spreading of information over the network. The attacker drops all of the received packets in blackhole attack, while drops some packets in the greyhole attack. In IEEE 802.11p, each node must be authenticated to be a part of the packets' route. In this case, the authentication process can deny the external attacker from initiating blackhole/greyhole attacks. However, the standard fails to protect the network from internal attackers [10]. The broadcast of warning packets could reduce the effect of attack because of the diffuse multiple copies over the network.

  Also, LTE-V2X is capable of eliminating external attackers by applying mutual authentication between UEs and the core network. In D2D communications when two UEs are located out of the network coverage, there is a possibility that UEs communicate with another UEs with revoked credentials because they are not provisioned by the core network. In addition, the internal attacker is possible in case of relay coverage scenario when the UE that is located at the edge of eNB coverage uses other UEs to relay the packets to eNB. In

this case, the relaying node could be an internal attacker that drops the received packets and blocks the communication with eNB.

- *Flooding attack*: The attacker sends a huge volume of packets to make victim node unavailable. The IEEE 802.11p MAC is vulnerable to flooding attack [19]. To initiate the attack, the attacker may exploit the binary exponential back-off scheme. Among the competing nodes, the winning node captures the channel by sending data constantly. Thus, it causes delay in transmitting data by forcing loaded neighbours to back-off for a long time. Another weakness in IEEE 802.11p MAC is network allocation vector field [19]. When there is a communication between two nodes, the nearby nodes update their network allocation vector based on the communication duration. During that period, all neighboring nodes stop transmission and only overhear for the channel. On the other hand, the attacker may transmit bogus message to cause errors in the transmitted packets. As a result of MAC authentication, the previous attacks could only be initiated by internal attackers.

  In LTE-V2X, there may be two potential techniques to initiate flooding attack against a specific UE [20]. First, the malicious node can use the resource scheduling information to transmit an uplink control signal when another node uses the channel to transmit its information. Thus, it causes a conflict at the eNB. Second, the UE is permitted to stay in active mode, but turn off its radio transceiver to save its power resource. During that mode, the UE is still allowed to transmit packets in urgent situations. However, the attackers can inject packets during that period to cause flooding attack.

  Moreover, each UE transmits periodically buffer status reports to eNB which are used for packet scheduling and load balancing [20]. Flooding attack could happen when the attacker impersonates other UE and sends fake reports that indicate larger data volume than in the real UE. As a result, eNB may stop accepting new requests for joining the cell because it thinks that the cell is fully loaded [20].

- *Jamming attack*: the attacker broadcasts signals to corrupt the data or jam the channel. Both IEEE802.11p and LTE-V2X physical layer is based on the orthogonal frequency-division multiplexing technology. In fact, a jammer requires to recognize the presence of

packets to launch jamming attack. However, current solutions cannot prevent jamming signals. Using directional antennas could minimize the effect of this attack and allow for vehicles to avoid the jamming area [11].

- *Coalition and platooning attacks*: a group of compromised nodes collaborate to initiate malicious activities such as blocking information or isolate legitimate vehicles [18]. For instance, when several internal attackers collaborate and initiate blackhole attack, it could affect the information delivery even with broadcast nature that it is supported by the IEEE802.11p. Also, these attacks are not only limited to blackhole but include any malicious behavior. In LTE-V2X, several compromised node could prevent the traffic from the node at the edge of eNB coverage.

Threats on Integrity

Ensuring the integrity includes the assurance of the accuracy and consistency of data that spreading over the network. The following attacks address data integrity:

- *Alter or inject false messages attack*: the compromised node spreads bogus messages in the network, by generating a new message or modifying the received one [21]. In both cases, it misleads the vehicles by giving them wrong information and putting them in a danger situation.

  In IEEE802.11p, it is possible that an internal attacker may try to broadcast false safety messages through the network. Broadcast messages are intended for all surrounding nodes, but they need to be signed in order to hinder external attackers from generating bogus messages. Because internal attacker is an authenticated node, it could use its digital certificate to sign any number of false messages [11]. However, the standard requires an additional scheme to be able to detect the attackers and include them in certificate revocation lists. In addition, these messages are protected from alternation because they are digitally signed by the sender's certificate.

In LTE-V2X, an external attacker cannot inject/alter any packet because the user data in LTE-Advanced is encrypted with ciphering key which is generated after a mutual authentication [20]. On the other hand, the internal attackers can inject false information in the network. Also, they can alter the received messages because in all communication scenarios the integrity algorithm is only applied on signalling packets.

- *Replay attack*: the compromised node captures the packets and replays them in a different time to look like that they were sent by the original sender. The vehicles which are operating in IEEE802.11p can defend against replay attacks where each node has a cache of recently received messages. Any new message is compared with the ones in the cache, and messages older than a predefined time are rejected [19]. To prevent replay attack, LTE-V2X uses a timestamp and a nonce in each message. Also, the message has a short lifetime in the network, which leads to reject any repeated messages [20].

- *Global Positioning System (GPS) spoofing attack*: the compromised node sends messages with fake location or after a period of time. In general, GPS is responsible for delivering both location and time to the surrounding nodes. However, GPS antennas are vulnerable to damage from storms and lightning. In addition, the antennas are susceptibility to jamming or spoofing attacks. In both protocols, the attackers can send fake location by generating strong signal from a GPS satellite simulator. Moreover, a successful replay attack could happen when UE uses GPS clock for message timestamp because it is easy for the attacker to spoof GPS clock [22]. Thus, the repeated message, which is sent after a while, could be accepted as a new message [11]. In this case, the protocols require to propose plausibility checks to detect fake location and time.

Threats on Confidentiality

The confidentiality requirement allows for information to be known only by the intended receiver. This is usually achieved by encrypting the message with the public key of the receiver where it only can be decrypted by the private key of the intended receiver. Some threats violate this requirement [23], such as:

- *Eavesdropping attack*: it aims to capture the packet's information and acquire sensitive and confidential information. Broadcast messages generally contain traffic safety information which are considered non-confidential information [19]. On the other hand, location based services and other types of transaction application information are encrypted in IEEE802.11p. As long as the internal attacker can collect information without a permission from other users, it considers a challenge.

  In LTE-V2X, the UEs use the pre-shared secret keys which are issued by the authentication center to establish a secure communication with the core network. Thus, the external attacker cannot collect information because the communication is encrypted. While in D2D communication, the UE use a pre-shared secret key for each application. However, this may cause additional computation costs on UEs [16]. In both communications, internal attacker can gather network information. To reduce the latency and computation cost, the message is not encrypted. As a result, the external attacker can also collect confidential information.

- *Location tracking*: sharing the location with neighboring nodes is very important for various vehicular applications. However, the attackers can collect and use these information for tracking users. In IEEE802.11p, every time an on-board unit broadcasts a message to warn neighboring vehicles regarding a safety update, it digitally signs the message with its own certificate. Therefore, the receiving nodes can identify the sending on-board unit and its current position. Unfortunately, wireless access in vehicular environment cannot support anonymous broadcast messages [11]. In LTE-V2X, the core network assigns different temporary identifiers, which are continuously changed, to UEs. The temporary identifier is sent to UEs in a plain text. Thus, the passive attacker is able to identify the location of the user at that time [20]. However, location tracking could be achieved only if the attacker can perform the mapping between various identifiers and the UE. As a consequence, both internal and external attackers can initiate that attack.

Threats on Authenticity

Ensuring the authenticity includes the process of giving nodes access to the network based on their identity using certificates and digital signatures. It works like a wall that protects the network from external attacks. Some threats violate this requirement [24] such as:

- *Certificate replication attack*: the compromised node uses replicated certificates to conceal itself by deleting the certificates that were added to the blacklist.
- *Sybil attack*: a single compromised node pretends many fake identities.
- *Masquerading attack or impersonation attack*: the attacker exploits a legitimate identity to obtain access to the network and confidential information.

Using fake identity in IEEE802.11p by the internal or external attacker could be prevented using certificate revocation lists. Each on-board units and RSUs can be identified by their certificate and in case that the normal node turns to behave maliciously, the identity will be added to the certificate revocation lists. In LTE-V2X, the home subscriber server is able to avoid the messages that come from unauthorized UEs by applying the mutual authentication. Thus, the user impersonation or sybil attack will also be prevented [25]. However, UEs are not protected when they are located out of the network coverage because they cannot ensure that they have the updated certificate revocation list.

Threats on Non-repudiation

Non-repudiation is responsible for identifying the real node's ID which performs a specific behavior. It is a method to ensure message transmission between entities via digital signature and/or encryption [18]. In IEEE802.11p, the periodic message and warning messages are signed with the sender certificate. Also, the location based services and any sensitive information are encrypted. Thus, the node identity can be identified when it launches a malicious behavior.

In LTE-V2X, the message exchange between UEs and eNB is encrypted with cipher key. In addition to the encryption, LTE-V2X applied integrity protection on the signaling packets.

Table 2.2: Comparison between IEEE802.11p and LTE-V2X regarding to security services

Security Requirements	**Threats**	**IEEE802.11p**		**LTE-V2X**			
				Cellular-based		D2D-based	
		External	Internal	External	Internal	External	Internal
Availability	Blackhole Greyhole attacks	Authentication scheme	N.P.	The mutual authentication between UE and the core network.	N.P.	N.P.	N.P.
	Flooding attack	Authentication scheme	N.P.	Authentication scheme	N.P.	N.P.	N.P.
	Jamming attack	N.P.	N.P.	N.P.	N.P.	N.P.	N.P.
	Coalition attack	The attack is only initiated by compromised nodes that are authenticated.	N.P.	Same tech. in IEEE802.11p	N.P.	Same as IEEE802.11p	N.P.
Integrity	Alter/inject messages attack	N.P.	Digital Signature	The user data in LTE-Advanced is encrypted with ciphering key which is generated after a mutual authentication.	N.P.	Same as cellular link	N.P.
	Replay attack	Each node has a cache of recently received messages	Same as external	It uses a timestamp and a nonce in each message + msg short lifetime	Same as external	Same as cellular link	Same as cellular link
	GPS spoofing attack	N.P.	N.P.	N.P.	N.P.	N.P.	N.P.
Confidentiality	Eavesdropping attack	Encryption scheme	N.P.	The UEs use the pre-shared secret keys which are issued by the authentication	N.P.	N.P.	N.P.
	Location tracking	N.P.	N.P.	N.P.	N.P.	N.P.	N.P.
Authenticity	Certificate replication attack	Certificate revocation lists	Same as external	The mutual authentication.	Same as external	N.P.	N.P.
	Sybil attack						
	Masquerading /impersonation attack						
Non-repudiation	Any	-	Encryption +Digital signature	-	Encryption +integrity on signaling pckts	-	N.P.

*N.P.: Not Protected.

On the other hand, it is very hard to ensure non-repudiation requirements in cooperative D2D communications because of trust concept. Indeed, if one node trusts another node, it communicates with it even if it used fake identity. Thus, that violates some features of non-repudiation [26].

Summary

A summary for the supported security services in each communication protocol is presented as shown in Table 2.2. As a conclusion, the D2D link in LTE-V2X is the most exposed link to external and internal attacks. The reason behind is that the D2D link is not managed by the core network when both nodes are located out of the network coverage. In contrast, IEEE802.11p has more security services which achieve more secured ad-hoc link between vehicles.

2.2.2 Security Solutions for V2X Communications

Vehicular communications encounter many challenges, therefore, ensuring a trusted communication is considered a complex function. Because of the shortage of the security services in both enabling technologies of V2X communications, an additional security model is needed to protect the vehicular network.

Here, various security solutions, that were proposed for vehicular networks, are presented. They are divided based on the security method into three categories: cryptography-based, behavior-based and identity-based. The outline of the proposed classification scheme is shown in Figure 2.6.

Cryptography-based solutions

Cryptography is responsible for achieving a secure communication between a sender and a receiver by developing algorithms that prevent unauthorized users from accessing the network [27]. As a result, these algorithms concentrate on external attacks that are launched by unauthorized users. *Encryption* is the main technique in cryptography-based solutions where it uses various algorithms to transform the data into another form that is only readable by intended users

[28]. For example, Li *et al.* [29] proposed a lightweight secure navigation system for VANET. Each vehicle applies encryption and the digital signature for supporting a secure communication between the vehicle and RSU. The system addressed the replay attack and man-in-the-middle attack. In addition, the proposed model in [30] applied advanced encryption standard to achieve the user privacy. The key distribution problem of advanced encryption standard was addressed by taking advantage of the randomness of the channel in vehicular networks to share the secret key. In addition, the secure and intelligent routing protocol in [31] used a double encryption for the data packets and applied authentication scheme to measure the node's trust. However, it caused an increase in the processing time and raised the network overhead.

Shukla *et al.* [32] proposed a model that obtains the security in the vehicular network using

Security Solutions	Cryptography-based solutions		Encryption	Li et al (2015), Abdelgader and Shu (2017), Bhoi and Khilar (2014), Shukla et al (2016)
			Key Management	Hong et al. (2008), Zhang (2017), Lei et al. (2017), Wan et al. (2016), Zhu et al. (2017)
			Authentication	Chuang and Lee (2014), Yang et al. (2017), Mamun et al. (2014), Ying and Nayak (2017), Sun et al. (2017)
	Behavior-based solutions		Weighted-sum	Gazdar et al. (2012), Kerrache et al. (2016b), Patel and Jhaveri (2015), Wei et al. (2014), Abdelaziz et al (2014), Golle et al. (2004), Yang (2013), Ding et al. (2010a), Dixit et al. (2016), Rostamzadeh et al. (2015) Li et al. (2013), Khan et al. (2015), Shen et al. (2013).
			Rewarding scheme	Haddadou et al. (2013), Haddadou et al. (2015), Jesudoss et al. (2015), Kerrache et al (2015)
			Fuzzy Logic	Marmol and Perez (2012), Rafique et al. (2016), Ding et al. (2010b)
		Other	Support Vector Machine	Fan et al. (2016), Kim et al. (2017)
			Rule-based	Sedjelmaci and Senouci (2015)
			Dempster Shafer Theory	Li and Song (2016)
			Subjective logic	Huang et al. (2017)
			Packet modification	Chen et al. (2010), Jahan and Suman (2016), Zhang et al. (2016)
			Heuristics-based	Wu et al. (2016)
	Identity-based solutions		Geographic proximity	Al Mutaz et al. (2013)
			Random pseudonyms	Shaikh and Alzahrani (2014), Kang et al. (2017), Raya and Hubaux (2007), Sun et al. (2010), Chen and Wei (2013)
			Group ID	Tajeddine et al. (2010)

Figure 2.6: Overview of the surveyed research works - Classified according to the security methods.

multiple operating channels where the encrypted data is sent on multiple channels. The receiver considers the mean value of the received data. For example, if the attacker hacks some channels and alters the data. Then, the partial incorrect data is received which is improved partially by taking the mean of the received data. Also, in case of jamming of particular channels, the receiver still can receive the data using other channels. However, this method is only considered when the security is a major concern rather than resources because it achieves a high bandwidth waste.

Key management process manages the cryptographic keys in a crypto-system which includes the generation, exchange and storage of the keys. For instance, Hong *et al.* [33] proposed a situation aware trust that is based on vehicle situations. For building the situation aware trust, first the attributes (static or dynamic), such as time, company and location, should be defined. The group which belongs to specific attribute share the same key. Then, the packet is encrypted using that key where it only can be read by the group members. For example, if there is a taxi from company A and wants to send a message to other drivers. The message has four attributes as follows (Company, Taxi, Time, Location). As a result, only vehicles with these attributes can read the message. Moreover, Ahmed and Tepe [34] proposed a novel method based on one-time identity-based authenticated asymmetric group key agreement to create cryptographic mix-zones which resist malicious eavesdroppers. The safety messages are encrypted using a group secret key to improve vehicle privacy. Thus, any external entity cannot track the safety messages in the cryptographic mix-zones. In addition, Lei *et al.* [35] proposed a novel key management scheme for key exchange among security managers in heterogeneous networks. They used blockchain concept for allowing key exchange securely within the security manager network. Flexible transaction collection period was proposed to reduce the key exchange time in blockchain scheme.

A key generation model in [36] used received signal strength to guarantee the randomness in key generation. The node senses the received signal and transforms the received signal strength values to binary value by applying upper threshold (Th_{up}) and lower threshold (Th_{low}). For key generation, the node sets one if the received signal strength value greater than Th_{up} and zero if the received signal strength value less than Th_{low}. Any value in between is ignored. Also, Zhu

et al. [37] proposed a scheme which gives the vehicles the ability to generate a shared secret key from received signal strength indicator values with low probability of getting the same key by neighboring vehicles.

Authentication schemes were proposed using various techniques to detect unauthorized nodes and prevent them from launching malicious attacks. For instance, Chuang and Lee [38] introduced a scheme for authenticating the vehicles by considering them trusted nodes if they are successfully authenticated. On the other hand, Yang *et al.* [39] proposed two lightweight anonymous authentication schemes for the V2X network. One scheme was applicable for V2V communication, while the other was suitable for V2I communications. Both schemes considered the limitations in V2X such as resource constraints of on-board unit and latency limit. Also, Mamun *et al.* [40] presented a reliable and standard chosen plain-text secure group signature solution for vehicular network applications. It allows any fixed entities such as RSUs to link messages, and recognize if they are generated by one or group of vehicles, without breaching their privacy. Thus, it prevents malicious complaints against normal nodes. In addition, Ying and Nayak [41] proposed an anonymous and lightweight authentication based on smart card protocol. It consists of two main phases which are user authentication and data authentication. It protects the network against various attacks such as offline password guessing attack, impersonation attack and many others. Also, the anonymity is achieved by using dynamic identities.

The work of [42] applied a model which is achieved the privacy and non-repudiation requirements. It is composed of two schemes which are identity-based signature and pseudonym scheme. Also, it provides the authentication in inter-vehicle communications.

Behavior-based/trust-based solutions

They were proposed as complementary solutions to cryptography, where traditional cryptography-based solutions are not able to detect internal attackers because they are authenticated users [21]. The trust evaluation is typically conducted by monitoring nodes, which monitor and collect other nodes' behavior information. The most common methods that are used for trust management in vehicular networks are as follows:

- **The weighted-sum method** is the most common methodology for trust management, where trust evaluation is computed by assigning different weights for each trust component. When the node behaves maliciously; the total trust value decreases until it reaches zero [43]. Total trust is computed by:

$$T_{total} = \sum_{i=1}^{U} w_i \times T_x \tag{2.1}$$

where w_i is a weight value for T_x, T_x is a trust value for trust level x such as direct and indirect. Direct trust measures trust level of one-hop neighbors using direct monitoring, while indirect trust measures trust level of two-hops neighbors using the recommendations from other nodes. U is the number of trust levels that are considered.

Gazdar *et al.* [44] proposed a dynamic and distributed trust model for VANET that used the monitoring nodes for observing their neighboring nodes and sending an alert about any malicious activity such as packet dropping or packet modification. On the other hand, Kerrache *et al.* [45] proposed trust model that provided two trust metrics: vehicle-based and RSU-based. Each node is able to monitor its neighbors and measure local trust value. Then, RSUs are responsible for managing a global and historical trust information about all nodes which locate in the same road segment. At the same time, the model could work without the existence of RSU. Patel and Jhaveri [46] applied ant colony optimization algorithm for choosing the shortest trusted path by isolating non-cooperative nodes. However, the node is compelled to transmit the packets to the next hop even if all neighbors are malicious. Unlike [46], Wei *et al.* [47] proposed a trust model for detecting non-cooperative nodes on V2V communications only. Moreover, Abdelaziz *et al.* [48] proposed intrusion detection system to enhance the message relay mechanism by evaluating the trustiness of received messages.

Event-based models collect data and monitor different events going on in the environment to build the reputation. In the vehicular networks, some models were proposed to monitor traffic events and evaluate the trustworthiness of these events. For example, event-based reputation model was proposed in [49] for checking data consistency. Indeed, the sensors

provide redundant information which allowed for each node to process the data and remove malicious information. If inconsistencies occur, the security model is activated to detect the malicious node. Furthermore, similarity mining technique was suggested in [50] for recognizing similarity among vehicles and messages. For instance, at a similar location and similar time, messages about the same event that are generated by the same vehicle usually have similar trust values. In addition, Ding *et al.* [51] proposed event-based reputation model to filter fake warning messages and increase the accuracy of the network. It measures the reputation of the event based on its roles (event reporter, event observer or event participant) to check if the event triggered is real or fake alarm. Furthermore, trust value can be related to a specific location. For example, when trustworthy interactions are established between vehicles in a specific road segment, then, the corresponding trust value for that location and time is increased. Dixit *et al.* [52] proposed a model for selecting the trusted location using Ad-hoc On-Demand Distance Vector (AODV) routing protocol where RSUs were responsible for controlling the packets routing. However, as the number of malicious nodes increased, the vehicles may follow the wrong path. In addition, the proposed framework in [53] is composed of two modules: the first one implements three security checks to measure the message's trustworthiness. First, it examines that the message is generated from a trusted location and followed a trusted route. Second, it inspects that the message route does not contain any malicious nodes. Third, it checks that it has a valid content. Indeed, it computes a trust value for each road section and for each neighborhood. Once a message is evaluated and considered trusted, then it looks up for a trusted route to forward the message.

The new malicious nodes behave intelligently and conceal themselves from detection by alternating between normal and malicious behaviors. To protect the network from smart attacks, Li *et al.* [54] offered a reputation-based global trust establishment to address a smart blackhole attack by considering the past behavior of nodes.

The monitoring role could be concentrated on the message content. The monitor nodes measure trust value based on the validity of the received messages. For instance, Khan *et al.* [55] proposed an algorithm for VANETs which provides distributed message authentication.

It gave the monitoring roles to specific nodes called verifier nodes. These nodes were responsible for verifying the message and transmitting the decision through the network. The model considered three parameters for choosing appropriate verifiers which are load, distance and trust value. In addition, Shen *et al.* [56] proposed a distributed authentication scheme where verifier vehicles were responsible for checking the validity of the message while non-verifier vehicles depend on verification results. The choice of verifier nodes is made using three methods: N-nearest method, most-even distributed method and hybrid method.

- **The rewarding-based method** uses credit to reward cooperative nodes. For instance, the node rewards its neighboring node while it behaves normally and cooperates with other nodes. Thus, a node with high trust value considered a reliable node. The rewarding method is used as a security solution to encourage non-cooperative nodes to participate in packet forwarding process. For example on this, [57] and [58] proposed a rewarding scheme for detecting blackhole and greyhole attacks. Also, Jesudoss *et al.* [59] proposed a payment punishment scheme where it is applied during election and routing processes. They used Vickery, Clarke and Groves model and designed the payments in a way that the collaborative node will gain rewards and be able to participate in election and routing processes. In addition, the model assigns the monitoring role to some nodes where they continuously monitor the behavior of relaying nodes. The work in [60] proposed trust-based routing protocol which is composed of two main phases. The first phase includes the trust measurement, which is done periodically and in a distributed manner. When the node receive a data packet, it applies trust model on the received packet. Thus, it is able to evaluate the sender behavior and compute its trust value. Then, based on the previous step, the second phase involves sending the data through the most trusted route.

- **The fuzzy logic method** incorporates a series of IF-THEN rules to solve a control problem rather than attempt to model a system mathematically. The main steps of the fuzzy logic model are as follows [61]. First, the fuzzy sets and criteria are defined; next, the input variable values are initialized; then, the fuzzy engine applies the fuzzy rules to

determine the output data and evaluate the results. For instance, Mármol and Pérez [62] proposed a security model that worked on detecting selfish nodes that transmit false or bogus messages. The model defined a fuzzy set to classify each node with three different trust levels. Based on the source node trustworthiness level, the receiver can decide whether it has to receive, forward or drop it. Also, fuzzy logic models were proposed in [63] to detect packet dropping attack. Moreover, Ding *et al.* [64] proposed a fuzzy reputation based model to prevent the spreading of false messages.

- **Other methods** Some existing models utilized different methods to detect internal attacks. For example, Fan *et al.* [65] proposed a detection system using support vector machine learning algorithm to stop replay attack. It applied a training phase to fetch attack's characteristics. In addition, Kim *et al.* [66] proposed collaborative security attack detection mechanism in a software-defined vehicular cloud architecture. It consists of two phases: *information aggregation phase* where each vehicle analyses the received information and transmits the result periodically to the controller for training the support vector machine, and *Multi-class support vector machine training phase*. Then, the classification using support vector machine starts where each vehicle applies the classifier to detect malicious nodes. However, this method is not energy-efficient because it requires training phase to be able to detect the attack. Sedjelmaci and Senouci [67] proposed a framework as intrusion detection system that concentrated on behavioral attacks. It addresses various attacks in VANETs such as selective forwarding, blackhole, wormhole and sybil attacks. It uses special agents which are responsible for monitoring the nodes' behavior and triggering an alarm when a misbehavior is detected. It is composed of two detections systems and decision system. First, local intrusion detection system which operates on each node to monitor its neighbors and the cluster head. Second, global intrusion detection system which runs at the cluster head level to monitor its cluster members. Finally, global decision system runs at RSU level to calculate trust level for each node by aggregating the reputation of each node and broadcast the blacklist through the network.

  In addition, Li and Song [68] proposed a model using Dempster-Shafer theory of evidence to combine multiple evidence even if some of them might not be accurate. It was proposed

to evaluate two types of trust: data trust and node trust. In particular, data trust is used to evaluate the received data and indicate if it is acceptable based on a calculated trust value. On the other hand, node trust assesses the node based on its behavior with neighboring nodes and indicates whether or not it is trusted.

A distributed reputation management system was proposed in [69] for securing vehicular edge computing. Vehicular edge computing servers were used to implement local reputation management tasks for vehicles. In addition, they applied multi-weighted subjective logic for computing the reputation values. On the other hand, some existing solutions implemented adjustments on existing routing protocols to increase the security level. For instance, in the model that was proposed in [70], each node appends a list of trust opinions with the cluster data. Also, it applies confidence level for its opinion to determine the assurance level about the computed trust value. Moreover, Jahan and Suman [71] proposed a change in routing protocol to detect non-cooperative nodes using a double acknowledge technique. In another work, Zhang *et al.* [72] proposed an amendment to AODV routing protocol to identify packet dropping behavior by adding new fields to the control packets. The main drawback of this method is the risen network overhead as a result of the increase in packet size.

Moreover, Wu *et al.* [73] proposed a lightweight anti-phishing application. They develop enhanced version of heuristics-based method by addressing the high relying on web page source code. They implemented it on a Google Nexus 4 smart phone running the Android 4.2 OS.

Identity-based solutions

They address attacks that exploit users' identity for malicious activities such as sybil attack and breach user's privacy. Most security solutions used the vehicles' identity to identify them and revoke malicious node. As a result, user's privacy has been revealed and misused by an attacker. To resolve this issue, the security model should operate on an identity anonymous environment. For example, Shaikh and Alzahrani [74] proposed the first trust management scheme which takes

into account the anonymous identity. It protects VANETs from spreading messages with fake location and time. Each node calculates its confidence value regarding the received messages about a specific event. The confidence value is based on four parameters: location closeness, time closeness, location verification and timestamp verification. Then, it calculates the trust value for each message that reporting the same event and makes the decision regarding that message based on the trust value.

Moreover, Tajeddine *et al.* [75] proposed a privacy-preserving trust framework that allowed for collecting information about vehicles' behavior while preserving their privacy by applying a group ID rather than real identity. Also, Chen and Wei [76] proposed a beacon-based trust model that ensures the VANETs safety while preserving the drivers' privacy. All transmitted messages were protected by cryptography and the pseudo identity schemes.

One common approach to preserve the privacy of vehicles' location is the use of pseudonyms. Indeed, the vehicle broadcasts its information with pseudonyms that frequently changes [77]. As an example of this, Kang *et al.* [78] proposed a system for defending two cases of eavesdropping. The first case, an adversary tracks a target vehicle by a specific pseudonym. In this case, the security solution used a random virtual machine identifiers which make the mapping relationship fail. Unfortunately, the first solution was vulnerable to identity mapping attack. Because of that, they proposed pseudonyms changing synchronization scheme to improve detection accuracy. In addition, Sun *et al.* [79] presented the VANET security system which based on three main techniques. First, a pseudonym-based technique which was used to assign pseudonym/private key pairs to the vehicles which are traveling in the home domain or other domains. Second, threshold signature which was applied to send the secret information for recovering a malicious vehicle's identity. Meanwhile, it prevents compromised nodes from having a full authority to revoke a normal node. Third, threshold authentication based defense scheme which provides a mechanism to distinguish between malfunctioning and malicious behavior.

Geographic proximity technique is used to detect sybil attack when the malicious node uses multiple identities. Al-Mutaz *et al.* [80] applied this method to identify sybil identities where

the geographic proximity of the compromised node and all its sybil identities last for a long time and repeated.

Summary

Here, a summary to get an overview of the proposed security methods is provided. Table 2.3 summarizes characteristics of the main security models were proposed for vehicular networks. The parameters of this summary are presented as follows:

- Organization: indicates whether the model applied on flat or clustered network.
- Architecture: indicates whether the model used the centralized structure, distributed or hybrid.
- Purpose: indicate whether the aim of the model is intrusion detection system, achieve a secure route or protect message content.
- Addressed attacks: indicates which attacks are addressed in the model.
- Security requirements: indicates which requirements are achieved by the model.

Table 2.3: Main security solutions in vehicular networks

	Topology					Purpose			Addressed Attacks			Security Requirements					V2X Comm. Type	
	Organization		Architecture (Use of RSU)			IDS	Secure Route	Secure Content	Internal attack	External attack	Both	Av.	Int.	Conf.	Auth.	NRep.	V2V	V2I
	Flat	Clustered	Centralized	Distributed	Hybrid													
[67]		✓	✓			✓			✓			✓	✓				✓	✓
[58]	✓			✓			✓		✓			✓					✓	
[53]	✓		✓				✓	✓	✓			✓	✓				✓	✓
[45]	✓				✓		✓	✓	✓			✓					✓	✓
[38]	✓			✓			✓	✓		✓			✓		✓		✓	
[81]	✓		✓					✓		✓			✓				✓	✓
[82]	✓				✓		✓				✓	✓				✓	✓	✓
[34]	✓		✓					✓		✓				✓	✓		✓	✓
[37]	✓			✓				✓		✓				✓			✓	
[79]	✓		✓			✓				✓				✓	✓	✓	✓	✓
[83]	✓				✓		✓				✓	✓					✓	✓
[35]	✓		✓			✓				✓			✓				✓	✓
[69]	✓			✓		✓			✓			✓			✓		✓	
[42]	✓		✓			✓				✓		✓		✓	✓		✓	✓

*Av: Availability, Int: Integrity, Conf: Confidentiality, Auth: Authentication and NRep: Non-repudiation

As a conclusion, much researches applied the security model on a flat network where all nodes have the same responsibility. In addition, many security solutions focused on addressing one type of attacks: internal or external. Also, using central units for security measurements was frequently used. However, centralized models are not applicable in vehicular networks where the node could be located out of the network coverage.

2.2.3 Discussion and Comparison

The effectiveness of security methods for protecting V2X communications is discussed in this subsection. Based on the proposed analysis, most of the proposed models were applied on vehicular ad-hoc network where the security model was implemented on vehicles (homogeneous network) only. Because V2V is part of V2X communications and both of them support the communications in vehicular network, they have common characteristics such as various speeds, non-stable connection and dynamic topology. As a result, studying the security solutions in V2V is required to address their challenges while designing security model for V2X communication. In addition, few proposed security models [55, 59, 67, 70] considered clustering vehicular network and all of them are behavior-based solutions. After analysing the existing solutions, Figure 2.7 represents the evaluation based on four parameters as follows:

- *The considered attack:* study the ability of various security methods in protecting the network against internal or external attacks.
- *The message type:* study to which extent the security method is important for delivering various V2X messages.
- *The latency limit:* study the effect of applying various security methods on message delivery time.
- *The security model structure:* study the impact of security method on the model structure.

The considered attacks

Some existing works in [31, 32, 38] used traditional security scheme for protecting vehicular networks such as encryption and authentication. These methods are important in protecting the network from external attacks, and also they achieved high-security levels in a centralized network. However, they are not reliable solutions for distributed networks. Moreover, based on the study on V2V applications which was done in [84], they listed some limitations of various cryptography-based methods. Symmetric key systems cause additional overhead and delay in key distribution phase. While, asymmetric cryptography is suitable for distributed systems where nodes are highly dynamic. However, it is slower than symmetric key systems and causes a huge latency. Furthermore, the revocation process in group signature method needs high computation power and also the signature is too large to transmit over the air.

Based on the previous comparison between the main vehicular network communication protocols, the most external attacks are considered by protocol security services. Thus, applying additional cryptography model will increase the overhead on the network.

Considered Attack	External Attack	Some existing works in [31,32,38] used traditional security methods for protecting network against external attacks. However, it causes a huge latency that decreases the network performance in V2X.
	Internal Attack	[85,86,18] proposed behavior-based solutions to fill the gap and protect the network against internal attacks. The weighted-sum method is the common method for vehicular network.
	Both	To ensure that the network is protected against both attacks, [82, 83] suggested solutions that implements traditional methods in addition to the behavior-based solution.
Message Type	Event-based Msg	As this type of messages requires to be delivered in very short time, the behavior-based solution were proposed in [44,53,55,62]. Also, the message content does not need to be encrypted.
	Periodic Msg	The content should be encrypted to prevent external attackers from tracking users. Also, some research [74,76, 87] proposed solutions to prevent internal attackers from mislead neighboring nodes.
	Unicast Msg	In most cases, this type of messages have personal and confidential information. Thus, the encryption for these messages are necessary.
Latency Limit	Time critical	For the messages that are delay sensitive, complicated models should not be applied on them.
	Not time critical	The messages, that are not delay sensitive, could use hybrid solutions (traditional + behavior-based) to protect the content.
Model Structure	Centralized	Most of encryption-based solutions applied centralized structure [34, 41, 79, 81]. However, centralized model is not suitable for vehicular network.
	Distributed	The distributed model could address the problem of central unit availability by giving each entity the ability to make its own decision. However, it lacks for global knowledge of malicious node in the net.
	Hybrid	The proposed model in [45] applied hybrid system which manages both model structures

Figure 2.7: Discussion for the proposed solutions based on four parameters

Behaviour-based solutions can be implemented as a supplemental solution to fill the gap of classical cryptography solutions, as proposed in [85, 86]. They are commonly necessary against internal attackers which they own legitimate certificates. Also, they are mostly applied on distributed and semi-centralized network [18]. The weighted-sum method has some challenges such as setting the weights and trust threshold, however, it is considered a common and computation-efficient method for vehicular networks. Because the vehicular networks require low latency in message delivery, a computation-efficient security method is recommended. Furthermore, there are few works that recommended fuzzy logic for the vehicular network, however, it needs a training phase and it is suitable for the predictable environment. On the other hand, the rewarding-based method is suitable for encouraging non-cooperative nodes. Therefore, it is limited to address the selfish behavior attack.

In addition, the shortcoming of identity-based solutions is the focus on attacks that exploit user's information to track them or pretend false identity. Thus, it is ordinarily used as complementary solution to protect user information where both protocols did not support anonymous identity. As a result, the need for designing identity-based solutions is increased.

Some researchers made efforts to address the previous limitation by applying a hybrid system, which combines multiple security methods to increase the security level of the network. For instance, Eiza *et al.* [82] utilized ant colony algorithm with graph model to detect internal attacks of routing control packets. It considers the external attacks by applying a digital signature. Also, it addresses internal attacks using plausibility checks such as QoS, link breakage and control messages broadcast. Also, Harsch *et al.* [83] suggested a security solution that combines distributed plausibility checks and digital signature technique. The model used time stamps, transmission range and vehicle's velocity to detect false position injection.

The message type

- **Event-based messages:** The message encryption is applied to keep the message content confidential while using multi-hop route. However, the encryption is not essential for event-based message because it is directed towards all nodes in the area and not targeting specific

destination. Thus, the message should be delivered to all nodes in a plain text to be able to read its content and make a decision regarding the traffic in a short period [84]. As a consequence, the encryption could affect negatively on the network performance. On the other hand, unauthorized nodes may start behaving maliciously and mislead other nodes by sending false messages. As a result, all nodes should be authenticated to be able to generate message to protect the network from false alarm which is injected by the external attackers. In addition, generating false alarm is not limited to external attackers but it can be initiated by authorized nodes. Much researches [44, 53, 55, 62] have proposed behavior-based solutions for securing packet content and detect internal attacker. The risk of tracking users by mapping event-based messages is too low because the road entity will generate a message when an event is triggered. Thus, the attacker can know the current location of the road entity but it has to wait for the next event to know its next location. As a result, hiding user's information is not critical.

- **Periodic messages:** The beacon message contains user's information such as location, speed and direction. This information is targeting on the nodes which are belonging to the network. Thus, this message should be encrypted to prevent external attacker from tracking users. Moreover, internal attackers may send false status information to mislead neighboring nodes. For instance, the model in [74] proposed to detect beacon messages with false location and time. Moreover, some recent works [76, 87] suggested beacon-based trust where the node's trust value is measured based on the validity of beacon message. As a result of missing mechanism in vehicular network protocols which protects user privacy, applying identity-based methods is necessary for beacon messages. The attacker can follow the beacon message and track the user's location because it is sent periodically and has much information about the user. Applying random identities is one of the main solutions for user privacy, however, it is vulnerable for mapping attack. The model in [78] proposed Pseudonyms Changing Synchronization Scheme to improve the user privacy.

- **Unicast messages:** In most cases, the unicast messages have personal and confidential information such as credit card. Thus, encrypting these messages are necessary to protect

users. Therefore, any nodes in the packet route cannot read the message content. In addition, to ensure the packet delivery, it should travel through trusted route to the core network. Thus, a behavior-based model is important to exclude any misbehaving nodes that try to drop these messages.

The latency limit

The vehicular network is latency sensitive where the information should be delivered to other nodes in short time, approximately 300 ms. As a consequence, applying complicated model will increase the delivery time. The main communication protocols for vehicular network support encryption and authentication services. Thus, applying additional cryptography solutions increases the packet delivery time. For instance, the model in [31] proposed double encryption scheme which increase the computation overhead.

Behavior-based solution were proposed as a computation-efficient solution, however, some research works [47] have proposed complex mathematical model to measure trust value. Also, some of these solutions applied machine learning algorithms such as support vector machine in [65, 66] where the complexity is high for training phase and testing phase. On the other hand, identity-based solutions are lightweight since they are only based on random pseudonyms [74, 76, 78, 79] or group ID [75]. These methods have simple calculations which do not require much time to apply them.

The model structure

Most cryptography-based solutions applied the centralized structure [34, 41, 79, 81]. However, the centralized model is not suitable for the vehicular network because the central units such as RSUs are not always available along the roadside. Because of that, [56, 88] proposed distributed authentication schemes. In addition, El-Zouka [88] proposed distributed authentication scheme where if the node would like to request a cloud service, it sends a message containing its own identity and its location to neighboring nodes; then, the neighboring nodes authenticate the message using a reputation list. However, it concentrated on V2V communication.

Behavior-based solutions are designed to give the nodes ability to manage security model independently from the central unit. However, some models used central units for gathering trust values from vehicles such as [52, 63, 67]. The main drawback in distributed structure is deficient in global knowledge about the network. For example, if *vehicle A* meets *vehicle B* for the first time, *vehicle A* does not have information about the security record of *vehicle B*.

The proposed model in [45] applied a hybrid system which manages both model structures. The distributed structure applied when the vehicles are located in the area that is not covered by a central unit. However, this assumption gives us non-stable detection accuracy.

2.3 The Proposed Solutions for Reliable Routing in V2X Communication

2.3.1 Reliable Routing Schemes in VANETs

The existing research were proposed to evaluate the link quality in VANETs. For instance, Eiza and Ni [89] applied the evolving graph theory to demonstrate the VANET communication. They developed a reliable routing scheme which supports QoS metrics in the routing process from the source to the destination. In addition, Li *et al.* [90] proposed an adaptive QoS-based routing for VANETs. It adaptively determines the intersections through which packets move to the destination. The selected route should obtain the best QoS metrics which are connectivity probability, packet delivery ratio and delay. Also, Fekair *et al.* [91] mentioned that the data routing in real-time and multimedia applications over vehicular networks is considered a challenge. Therefore, a multi-constraint routing algorithm was proposed to select the best path which achieves QoS requirements such as required bandwidth, maximum delay and jitter, and minimum link expiry time. Also, Sun *et al.* [92] suggested an adaptive routing protocol based on QoS and vehicular density in urban VANETs environments. It assists vehicles to find the best path which meets QoS requirements such as hop count and link duration. In addition, Liu *et al.* [93] presented quality of forwarding based reliable geographic routing for urban VANETs. It was proposed to find the best routing path that guarantees the quality of forwarding while providing

link reliability. It considers the transmission cost and the packet delivery ratio. Also, Also, Alzamzami and Mahgoub [94] designed a novel routing protocol based on fuzzy logic systems. It considers various metrics such as vehicles' position, direction, link quality, and achievable throughput to choose the most suitable relaying node.

Some works proposed an improvement in existing routing algorithms to achieve QoS in VANETs. For example, Toutouh *et al.* [95] defined an optimization problem to adjust the optimized link state routing protocol to be used in VANETs. They addressed the optimal parameter by using an automatic optimization tool. Also, Bitam and Mellouk [96] suggested a topology-based algorithm which supports the QoS for VANETs. It is based on ideas of the autonomic bee communication in the search behavior for the food. Also, Fekair *et al.* [97] proposed a QoS-based unicast routing protocol for vehicular networks. It consists of two phases: a clustering phase which manages the exchange of the routing information based on QoS requirements, and a routing phase which applies an artificial bee colony algorithm to determine the best route based on QoS criteria. Also, Eiza *et al.* [98] employed the situational awareness concept and an ant colony system-based algorithm to propose a situation-aware routing algorithm which supports QoS for VANETs. It was proposed to evaluate potential paths between two vehicles subject to multiple QoS constraints and choose the best-computed path. In addition, Moridi and Barati [99] offered a reliable multi-level routing protocol based on clustering in VANETs. In the first level, fuzzy logic was applied to improve AODV routing between cluster members. The fuzzy logic inputs were chosen to define the best and most reliable links. In the next level, the best link was selected between cluster heads via a search through a tabu list. Eiza *et al.* [82] employed the ant colony optimization technique to evaluate possible routes in VANETs subject to multiple QoS constraints determined by the data traffic type. The ant colony optimization rules are designed to consider the dynamics of the vehicular network topology. Also, Zhang *et al.* [100] used a genetic algorithm to propose a QoS routing protocol which achieves the QoS requirements during the link establishment between vehicles in VANET. However, the proposed solutions only support ad-hoc communications between vehicles.

2.3.2 Reliable Routing Schemes for Gateway Links between VANET and LTE

Recent research focuses on proposing schemes for choosing the best gateway between VANET and LTE. For instance, Chekkouri *et al.* [101] suggested a gateway selection scheme to relay the traffic toward the base station. The evaluation criteria are related to the received power and the existence in the RSU range. In addition, Wu *et al.* [102] offered a two-level clustering approach. The first level applies fuzzy logic to determine the cluster heads. It considers three factors which are velocity, leadership and signal quality. The second level utilized Q-learning algorithm for choosing which cluster heads can act as a gateway between V2V and LTE. Moreover, Zhioua *et al.* [103] suggested an algorithm for selecting the gateway based on fuzzy logic. The algorithm is a multi-criteria and QoS-based scheme. The criteria are based on the received signal strength, the load of cluster heads and the candidate gateway and link duration. In addition, Ucar *et al.* [104] suggested a hybrid architecture combining IEEE 802.11p-based and LTE with the goal of obtaining a high data packet delivery ratio and low delay while keeping the usage of the cellular architecture at a minimum level. The cluster head selection using various mobility metrics such as the average relative speed with respect to the neighboring vehicles and cluster connection time. Also, Mir *et al.* [105] proposed a location-based routing scheme for integrated VANET-LTE hybrid vehicular networks. In the proposed routing scheme maintaining local neighbor information and forwarding state results in fewer route requests to be sent towards the remote routing server. Then, the remote routing server calculates the route and sends the route updates to all intermediate vehicles on the path. But, it is based on centralized server to set-up the routes. However, all of the previous solutions were proposed to support the communications between two different networks.

2.3.3 Reliable Routing Schemes in LTE-A Networks

Some research developed ad-hoc communication for load balancing or range extending. For instance, Liu *et al.* [106] offered a D2D communication load balancing algorithm where the D2D device uses D2D relay node to deliver its packets to eNB in case of congested cells. Also, Liu *et al.*

[107] suggested D2D a communication-based algorithm to improve the quality of experience in LTE-A. However, they mentioned that most of D2D communication algorithms did not take into account the speed and directions while choosing the best D2D relay node. In addition, Tata and Kadoch [108] proposed a multi-path routing algorithm for direct communication in heterogeneous networks. It is an improvement of ad-hoc on-demand multi-path distance vector scheme which evaluates the available bandwidth while choosing the best route. Bastos *et al.* [109] suggested a network assisted routing algorithm in 5G to make a decision regarding the best link to the base station. The link evaluation is based on the number of hops and the channel quality. It was suggested to balance the load on various base stations. In addition, Yang *et al.* [110] designed a D2D bearer control architecture for D2D communications in LTE–A infrastructure. The data offloading decision is made by eNB or above. Then, eNB notifies the candidates that they have to conduct a discovery process. As the UEs come into the proximity of each other, the D2D session is switched to a D2D link. When the path is no longer available, they switched back to the cellular link. Also, Munir *et al.* [111] proposed a distributed relay selection mechanism that allows for a UE to act as a relaying node for the isolated UEs. It considers the link capacity and the relay's radial velocity. Also, Chi *et al.* [112] suggested an efficient reliable multicast scheme that employs D2D communication and network coding together to achieve high reliability. It was designed to address the challenging issues like node mobility, relay selection, D2D link selection, D2D retransmissions reduction, and acknowledgment implosion. However, most of the proposed solutions ignore the node mobility which has a high impact on the choice of D2D relaying nodes.

2.3.4 Discussion and Comparison

Here, the proposed solutions for direct communication in vehicular networks that consider QoS are discussed. Based on the proposed analysis, most of the proposed models were applied on vehicular ad-hoc network where the channel model is different than LTE-V2X. After analysing the existing solutions, the evaluation is done based on two parameters as follows:

- *The node characteristics:* study how various node characteristics affect on link quality .

- *The communication link:* study to which extent the communication type has impact on designing QoS-based model.

Node characteristics

Some research proposed relay selection models which achieve QoS requirements in LTE-A. They consider the protocol specification while designing the model, however, most of them were applied on previous releases. As a result, the mobility is considered for rare situations of high fast nodes where smart phones or tablets are mainly considered. As a result, the link has less outage probability than if the nodes are miving with high speed such as vehicles.

In addition, some research applied their models on VANETs which support IEEE802.11p. The vehicles have different specifications because of different protocols in comparison with LTE-V2X. For example, the transmission power in IEEE802.11p, which is equal to 37 *dbm*, is more than the one in LTE-V2X. As a result, the signal has more chance to arrive to the next hop because of high power. Also, the link data rate in IEEE802.11p is less than LTE-V2X. Thus, the transmission time for packets takes more time in IEEE802.11p. Therefore, it has more chance for delay in transmission.

Communication link

Based on the previous subsection, the communication link could be ad-hoc link in VANET as in [89, 93, 97], D2D as in [106, 108, 111] or gateway link as in [101, 103–105]. In the first case, the communication link works based on IEEE802.11p protocol which has different transmission power and frequency as presented above. The second case, where the communication link is D2D, the considered nodes are not vehicles. Thus, it leads to high difference in link quality. Final case, only some nodes work as a gateway, thus, all surrounding nodes send their packets to gateway nodes. Therefore, it causes a congestion and delay which is the worst thing could happen in the frequent change topology as vehicular network.

2.4 Challenges and Research Gaps

The trusted communication in the vehicular network is still considered an open research area. VANETs gave researchers the opportunity to study and evaluate their works. As a part of communication progress, the future vehicular network will not be limited to vehicles and RSUs, but it will include all roadside entities. As a result, applying traditional solutions in the V2X network cannot perform as it is expected.

Major efforts have been made; however, several open issues are still needing more consideration to achieve a trusted communication in V2X. Some of these issues are discussed in the following section.

Gap 1: Security attacks

1.1. In trust-based solutions, the evaluation is based on monitoring neighbor's behavior. As a result, they are susceptible to trust attacks, such as whitewashing attack, on-off attack and good/bad mouthing attacks. In these attacks, the compromised node behaves smartly to conceal itself from being detected by alternating between normal and malicious behaviors. Unfortunately, most existing works did not address them in vehicular networks except the proposed model in [54] that considered intelligent compromised nodes which behave maliciously for intermittent periods.

1.2. The wireless communication is the prospective method to facilitate the communication inside large public transportation systems such as trains, metro and buses. However, it is more susceptible to various cyber-attacks than the wired communication. Therefore, implementing security models for intra-vehicle sub-network is recommended. For instance, Liyanage *et al.* [113] proposed a secure system based on host identity protocol. It is designed to protect intra-vehicular communication from common IP based attacks.

1.3. Most centralized security solutions used RSU as a fully trusted unit for updating security records. Thus, the vehicles require communicating with RSU to get updated information.

However, this assumption is not applicable in vehicular networks because RSUs are not always available along the roadside. Also, RSUs, like any road entities, are vulnerable to various attacks [5]. As a result, in case of RSU attacks, these solutions are not working efficiently and have a huge impact on network performance. For instance, [114] developed security protocols for the key distribution, which are able to detect the compromised RSUs and their collusion with the malicious vehicles.

1.4. Most of traditional security solutions were applied on central units. On the other hand, many distributed solutions were proposed for vehicular networks to improve the decision accuracy. For vehicular network, the distributed solution is more efficient than the centralized one. However, the nodes are lacking of global knowledge regarding all untrusted nodes in the network. As a result, hybrid decision system is required for vehicular networks.

Gap 2: Security vs. QoS management

2.1. The term QoS is used to represent the level of performance provided to users. In traditional networks, high levels of QoS can be obtained by resource allocation and sufficient infrastructure. However, the control over the network resources, such as bandwidth, equipment, power consumption and transmission delay, is difficult in the vehicular networks because the network lacks of consistent infrastructure and stable topology. For instance, Wang *et al.* [115] proposed a method to fuse vehicle spacing information and estimate average traffic density. However, some security mechanisms can be added to the message frame to prevent attack on the spacing information. Therefore, achieving the trade-off between QoS and security level in vehicular networks is an essential task. The security model should always consider the efficient use of devices' resources because the road entities in V2X communication have various capabilities and resources. An example of this is the power consumption, all current security models did not consider the power consumption as a challenge because they were implemented on vehicles which have a long life battery. However, in V2X, some road entities such as mobile phones have a limited battery. As a result, designing a security model, that is computationally efficient, is recommended for V2X.

2.2. QoS includes the useful use of the network resources such as the bandwidth. Indeed, Zheng *et al.* [116] proposed a two-stage delay-optimal scheme by integrating software defined networking and radio resource allocation into an LTE system for vehicular networks. Also, the proposed model in [32] used multiple channels to send the same information which achieves the availability but wastes the bandwidth. In addition, the proposed models in [71, 72] caused further overhead by increasing the packet size. For critical applications such as safety-related applications in vehicular networks require a minimum delay for delivering warning messages to obtain a high safety level. However, most encryption methods need a time for encryption and decryption processes. Thus, they protect the information and achieve confidentiality but they have a negative impact on the QoS.

2.3. The existing solutions did not take into account the environment in the simulation model such as if the road is highway or urban. Also, they did not simulate the real propagation and mobility parameters which are affected by various factors such as signal fading, multi-path propagation and obstacles. Therefore, lack of applying models which simulate the real environment affects the performance metrics. In addition, existing security solutions did not consider the malfunction behavior or communication condition when making a decision about malicious nodes.

2.4. Finally, edge computing was applied on IoT-devices to allow data to be processed near to where it is created rather than crossing long route to reach the central server/cloud. Thus, it reduces the delay that is resulting from the packets transmission. Edge computing has been applied on V2X communication which is called vehicular edge computing because it works efficiently with latency-sensitive use cases. This is suitable for situations that require very short latency such as warning messages. However, security and privacy are still serious challenges in vehicular edge computing that require to be considered in the future [117].

Gap 3: Communication link quality

3.1. The link quality in vehicular network is still a challenge. The high speed nodes cause short connection time between nodes, and the existence of obstacles such as buildings or large trucks

could lead to intermittent communication. As a result of unstable connection, the packet should be delivered in a short time. The existing models applied on different communication protocols such as IEEE802.11p which cannot be directly used in LTE-V2X. The road entity in LTE-V2X has higher data rate and lower transmission power which cause a difference in evaluating the link.

3.2. Some research focused on choosing gateway node which link VANETs with LTE-A. The selection criterion for a gateway node is different than the selection of a relaying node. In addition, the link could be disconnected until the gateway selection round comes again. Also, many nodes choose the same node to relay their packets which causes buffer overflow or high queuing time. In both cases, the vehicular network is negativity affected. Therefore, designing a QoS-based relay selection algorithm is recommended.

2.5 Link between the gaps and thesis chapters

The existing works, that were presented to evaluated the communication link in vehicular networks, are mainly focus on VANETs where IEEE802.11p protocol is applied. However, IEEE802.11p has different network structure and link characteristics than LTE-V2X. Therefore, Chapter 3 proposed an algorithm for choosing the most reliable link in LTE-V2X which addresses Gap 3.1. In addition, few research suggested algorithms to choose the best gateway link between LTE-A and IEEE802.11p. However, the choosing criteria is not as choosing next relaying nodes. To solve the gap 3.2, Chapter 3 implemented a new multi-metric algorithm with the most important criteria in vehicular network.

Gap 1.1 is mainly focus on detecting non-stable malicious behavior where the compromised node starts malicious behavior in intermitted intervals or targets a group of normal nodes. In vehicular network, this type of attack becomes very hard to detect as the node can travel to different area (with new neighbors) each time interval. Therefore, Chapter 4 proposed a new trust model algorithm that implement recommendation filtering. It is able to detect non-stable malicious behavior as the recommendations from neighboring nodes are considered.

The existing trust models in vehicular network were proposed as a central or distributed models. In centralized models, the node depends on RSUs in updating or delivering trust values to the other nodes in the network. However, they always assume RSUs are trustworthy entity. Thus, Chapter 5 proposed a global roaming trust model that assume non-trusted RSUs that could start malicious behavior. The proposed model is able to minimize the impact of malicious RSU and road entities.

Moreover, in a very dynamic network as vehicular network, the nodes could communicate with a new group of road entities each time. Thus, a global knowledge regarding all malicious nodes in the network is recommended. Chapter 5 address this gap by implemented a global decision system in the central unit.

2.6 Summary

The rapid evolution of the transportation sector has caused security and trust challenges, which made the vehicular network vulnerable to various cyber-attacks that hinder the trusted V2X communication. Also, the features of the V2X network should be considered while designing the security model. In addition, the trusted communication link is one of the leading research gaps in LTE-V2X, which needs to be addressed.

In this chapter, the key features and architecture of the V2X network were defined. Also, the threats analysis for V2X enabling technologies was presented. Then, the current security solutions in vehicular networks based on the security method were analyzed. Also, A classification of the existing solutions for evaluating communication link in V2X was discussed. Then, the evaluation was done based on two main parameters, which are the node characteristics and communication link. Finally, the main challenges and future research directions were discussed for novel contributions to this research area.

Chapter 3

Multi-Metric QoS-balancing Relay Selection Algorithm in V2X Communications

This chapter achieves thesis aim by proposing a QoS-balancing algorithm for choosing the most trusted link. The proposed algorithm for LTE-V2X achieves Objective 1 in Chapter 1. Thus, it addresses various research gaps in Chapter 2, which are Gap 3.1 and Gap 3.2.

The vehicular network is a very challenging domain for supporting multi-hop communications because of frequent changes of its topology. Therefore, ad-hoc communications face various limitations such as connection time, channel capacity and signal quality. Based on literature review in Chapter 2, much research focused on supporting reliable connection for V2V links in VANETs [89–93] which have different link and network specifications than LTE-V2X. For instance, the link bandwidth in IEEE802.11p is less than LTE-V2X, however, the transmission power in LTE-V2X is lower than IEEE802.11p. Therefore, the link evaluation is changed based

on the communication protocol and network structure. Moreover, few research worked on evaluating communication link in LTE network [106–109, 112], however, the proposed solutions were implemented in previous releases of LTE where the node moves with a slow speed in comparison with the vehicular network. The node speed has high impact on link quality that should be considered while choosing the most reliable link. As a result, this chapter proposes an AHP-based algorithm for a trusted communication link in V2X. The link evaluation is based on three factors, which are link stability, channel capacity and end-to-end delay. The outage behavior probability is investigated for LTE-A (release 14). Finally, the performance of the proposed model is assessed by comparing it with the existing model [102].

3.1 Proposed System Model

The considered network is a V2X network with various numbers of road entity, which are vehicles, motorcycles, cycles and pedestrians, and RSUs. Here, "node" and "road entity" are used interchangeably for the same meaning. Also, the considered messages are the ones that should be delivered to eNB such as Internet services for updating maps, downloading a video or doing a transaction.

3.1.1 The Considered Scenarios

The road entity may need to use a multi-hop route to deliver its packets to the nearest eNB in some cases such as:

1. The road entity has a connection with eNB but the signal could become weaker because of the long distance between UE and eNB or the existence of obstacles. Then, the road entity decides to establish a D2D link with one of its neighboring entities to relay the packets to eNB.

2. The road entity does not have a connection with eNB. Thus, the road entity establishes a D2D link with a suitable neighboring entity to relay the packets to eNB.

3. The road entity could be in the network coverage but it uses a multi-hop route to reduce the cell load.

In the proposed model, the second scenario is the considered one to establish D2D communication.

3.1.2 Path-Loss Model

The actual channel state is affected by obstacles such as buildings, trucks and pedestrians. In addition, the vehicle's movement has a high impact on the transmission environment. Therefore, these factors are considered in the channel model. Based on literature review [118, 119], the validity range for path loss models in rural environments is greater than 10 $meters$. The average path-loss in dB, when the distance $d_{i,j}$ is greater than or equal to $10m$, is computed as

$$\begin{aligned} PL(d_{i,j}) = 20\log_{10}(\frac{40\pi d_{i,j} f_c}{3}) + min(0.03h^{1.72}, 10)\log_{10}(d_{i,j}) \\ - min(0.044h^{1.72}, 14.77) + 0.002\log_{10}(h)d_{i,j} \end{aligned} \tag{3.1}$$

where h is the average building height, and f_c is the center frequency in Hz where the frequency is equal to 700 MHz. The shadowing factor is $\sigma_{SF} = 4\ dB$ [118].

3.2 Multi-Metric QoS-balancing Relay Selection Algorithm in V2X Communications

A model for electing trusted links which achieves a high QoS is proposed. The proposed model applies the AHP on the road entity level for making the decision regarding which communication link is a trusted one. AHP is a multi-metric decision-making algorithm that utilizes a hierarchical approach to assess potential factors [120]. As most of multi-metric algorithms are complicated and not computation-efficient such as fuzzy logic, the AHP algorithm was chosen to implement the relay selection algorithm in V2X. Thus, Any delay in taking a decision could decrease the network performance. It combines qualitative and quantitative factors in the analysis. The analysis can be divided into the following four steps:

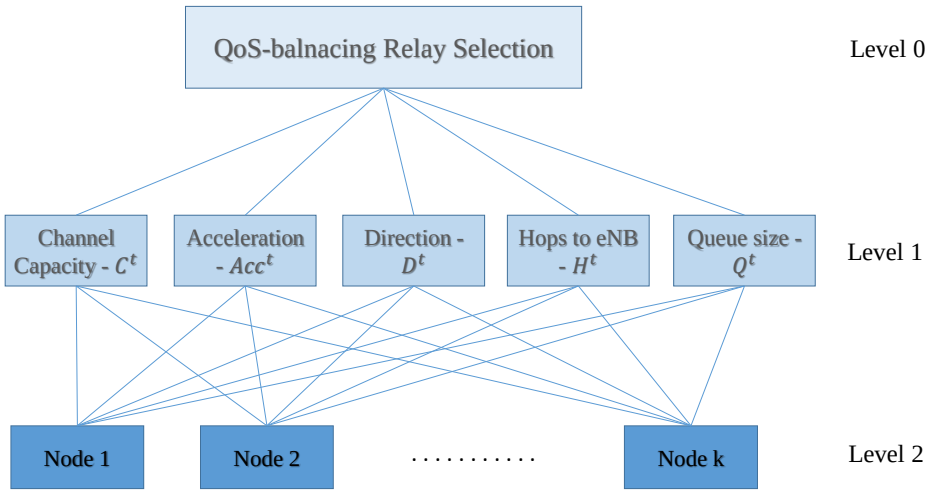


Figure 3.1: Structure of the proposed algorithm for QoS-balancing relay selection

3.2.1 First: Build a Hierarchical Model

The hierarchical model is constructed based on five criteria in level 1 as shown in Figure 3.1. Level 2 represents the potential links. For evaluating these criteria, the computed values are filled in a matrix as follows:

$$A = \begin{bmatrix} C_1^t & D_1^t & H_1^t & Acc_1^t & Q_1^t \\ : & : & : & : & : \\ : & : & : & : & : \\ C_m^t & D_m^t & H_m^t & Acc_m^t & Q_m^t \end{bmatrix} \tag{3.2}$$

where m is the number of potential links. The metrics are selected based on the most important ones in the related work [91, 108]. Also, the link stability and delay criteria are chosen based on the network requirements. The detailed information and calculation of the five factors are described as follows.

Channel Capacity (C^t)

As the connection time between two road entities is limited, a high channel capacity is required to guarantee the packet delivery. Three parameters are studied where they affect the channel capacity which are shadowing, multi-path propagation and signal noise.

First, the received signal power is measured with the impact of shadowing and multi-path propagation using [119]

$$RP_j(d_{i,j}) = TP_i - (PL(d_{i,j}) + X_{\sigma_{SF}}) \tag{3.3}$$

where RP_j is the received signal power at receiver node j with distance $d_{i,j}$, TP_i is the transmission power with which node i transmits a signal. $X_{\sigma_{SF}} \sim N(0, \sigma^2_{SF})$ is a random shadowing effect with a normal distribution with zero mean and σ^2_{SF} variation. Second, the SNR in dB is computed by

$$SNR_{dB_{(i,j)}} = RP_j(d_{i,j}) - P_{Noise} \tag{3.4}$$

where P_{Noise} is the noise signal in dB. SNR is computed by

$$SNR_{(i,j)} = 10^{\frac{SNR_{dB_{(i,j)}}}{10}} \tag{3.5}$$

Finally, the channel capacity in bit per second is calculated by applying Shannon's formula as follows

$$C^t = B \log_2(1 + SNR_{(i,j)}) \tag{3.6}$$

where B is the bandwidth of the channel.

Link Stability

The network topology in the vehicular network changes frequently. Thus, the communication link between two road entities is not always available. Link stability is defined as how long the link lasts between two road entities. Therefore, if the link stability is high between two road entities that could minimize the Packet Dropping Rate (PDR). It is evaluated by two main parameters as follows.

- **Acceleration (Acc^t):** is the rate of change of velocity of the road entity with respect to time t. Each road entity i computes the difference between its acceleration and the acceleration of the neighbouring entities j. It is computed by

$$Acc^t = \mid a_i^t - a_j^t \mid \tag{3.7}$$

  where a_i^t and a_j^t are the acceleration of node i and node j during a period of time (Δt), respectively. The relative acceleration of each node x is expressed as

$$a_x^t = \frac{v_x^t - v_x^{t-\Delta t}}{\Delta t} \tag{3.8}$$

  where $x \in N$ and N is the list of road entities. v_x^t and $v_x^{t-\Delta t}$ is the velocity of node x during current time t and previous time interval $(t - \Delta t)$, respectively.

- **Direction (D^t):** when the road entity establishes a connection with another road entity which is moving in the same direction, it gives them higher stability than when they are moving in the opposite directions.

As a result, when two road entities are moving with very close speed and in the same direction, it increases the link stability between them and reduces the chance of packet dropping.

End-to-End Delay

To increase the QoS of V2X networks, a minimum end-to-end delay for packet delivery is required. As the road entity sends packets through a multi-hop route, it is necessary to have a response in a short time. Therefore, two main parameters are considered while choosing trusted links which are:

- **Hops to eNB (H^t):** it is the conventional node-based routing metric that was used to select a route with less number of hops among the available routes to eNB. Most of the routing protocols in vehicular networks use hop count as their base metric. As an

assumption, each neighboring road entity sends this value to the neighbouring road entities to determine the shortest route to eNB.

- **Queue size (Q^t):** the queue size of the next hop entity is evaluated to prevent buffer overflow which causes eventually to high PDR. In addition, it is important to minimize the delay in queuing time. Therefore, the road entity prefers to choose the node with low queuing size.

3.2.2 Second: Form Pairwise Comparison Matrix (PCM)

Each element in the criteria level is compared with the other elements. The scale of numbers in Table 3.1 are used to determine the importance of one element over the other elements [120]. In Table 3.2, the diagonal line in the PCM matrix is filled by 1 because the criteria is the same where they are equally important. Also, when $y = 1$ and $u = 2$, the value is equal to 6 which means channel capacity C^t is strongly important in comparison with direction D^t. The values of Table 3.2 is filled in a matrix for further calculations as follows

$$PCM = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ : & : & : & p_{2n} \\ : & : & : & : \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{bmatrix}, p_{yy} = 1, p_{uy} = 1/a_{yu}, p_{yu} \neq 0 \tag{3.9}$$

where n is the number of criteria.

3.2.3 Third: Measure the Weight Vector of Decision Factors

The normalized relative weight matrix (B) is measured by dividing each element of the matrix (A) with the sum of its column

$$B = Normalize(A). \tag{3.10}$$

The normalization of matrix A is computed as follows

Table 3.1: 9-points scale for PCM [120]

Scale	Factors importance
1	Equally important
3	Weakly important
5	Strongly important
7	Very strongly important
9	Extremely important
2,4,6,8	Intermediate value between adjacent scales

$$Normalize(A) = \begin{bmatrix} \frac{C_1^t}{\sum_{v=1}^{m} C_v^t} & \frac{D_1^t}{\sum_{v=1}^{m} D_v^t} & \frac{H_1^t}{\sum_{v=1}^{m} H_v^t} & \frac{Acc_1^t}{\sum_{v=1}^{m} Acc_v^t} & \frac{Q_1^t}{\sum_{v=1}^{m} Q_v^t} \\ : & : & : & : & : \\ : & : & : & : & : \\ \frac{C_m^t}{\sum_{v=1}^{m} C_v^t} & \frac{D_m^t}{\sum_{v=1}^{m} D_v^t} & \frac{H_m^t}{\sum_{v=1}^{m} H_v^t} & \frac{Acc_m^t}{\sum_{v=1}^{m} Acc_v^t} & \frac{Q_m^t}{\sum_{v=1}^{m} Q_v^t} \end{bmatrix} \tag{3.11}$$

After that, matrix Y represents the importance degree of alternatives (potential links). Then, the potential link with the highest importance degree is chosen as the trusted link. Y is computed by

$$Y = B.\overrightarrow{ePCM} \tag{3.12}$$

where $\overrightarrow{ePCM}$ is the eigenvector of PCM. It is computed using the following equations where u

Table 3.2: Pairwise Comparison Matrix

Criterion	C^t $(u=1)$	D^t $(u=2)$	H^t $(u=3)$	Acc^t $(u=4)$	Q^t $(u=5)$	Priority Vector
C^t $(y=1)$	1	6	2	8	4	21%
D^t $(y=2)$	1/6	1	1/4	3	1/3	4.75%
H^t $(y=3)$	1/2	4	1	6	2	13.5%
Acc^t $(y=4)$	1/8	1/3	1/6	1	1/5	1.825%
Q^t $(y=5)$	1/4	3	1/2	5	1	9.75%

represents the column index, and T is the normalized relative weight matrix of PCM

$$\overrightarrow{S} = \begin{bmatrix} \sum_{u=1}^{n} T_{1u} \\ \sum_{u=1}^{n} T_{2u} \\ \sum_{u=1}^{n} T_{3u} \\ \sum_{u=1}^{n} T_{4u} \\ \sum_{u=1}^{n} T_{5u} \end{bmatrix} \tag{3.13}$$

Then, $\overrightarrow{ePCM}$ is measured by dividing each element in vector $\overrightarrow{S}$ by the number of criteria as follows

$$\overrightarrow{ePCM} = \begin{bmatrix} \frac{\overrightarrow{S}_{11}}{n} \\ \frac{\overrightarrow{S}_{21}}{n} \\ \frac{\overrightarrow{S}_{31}}{n} \\ \frac{\overrightarrow{S}_{41}}{n} \\ \frac{\overrightarrow{S}_{51}}{n} \end{bmatrix} \tag{3.14}$$

3.2.4 Fourth: Make a Consistency Test for the PCM

The consistency is expressed by the following equation, and the measure of consistency is called the consistency index [120]

$$CI = \frac{\lambda_{max} - n}{n - 1} \tag{3.15}$$

where λ_{max} is the maximum eigenvalue of PCM [120]. The random inconsistency [120] is computed by

$$RI = \frac{1.987 \times (n - 2)}{n}. \tag{3.16}$$

Finally, the consistency ratio is computed as

$$CR = \frac{CI}{RI}. \tag{3.17}$$

In AHP algorithm [120], if the value of the consistency ratio is smaller or equal to 10%, the inconsistency is acceptable [120]. If the consistency ratio is greater than 10%, resetting the

values of PCM is required. In the proposed model, the consistency ratio value is equal to 2.96% which is an acceptable ratio.

3.3 Outage Behavior Probability

3.3.1 Channel Capacity

The outage probability of a communication channel is the probability that a given data rate is not supported because of variable data rate. Outage probability is defined as the probability that data rate is less than the required threshold data rate. The required threshold data rate (R) is computed using

$$R = \frac{PcktSize}{time_{trans}} \tag{3.18}$$

where $PcktSize$ is the packet size and $time_{trans}$ is the required transmission time. Here, the outage probability of the communication channel is studied. The probability is computed as follows

$$\begin{aligned} P_{out}[C < R] &= P[C < R] \\ &= P[B\log_2(1+SNR) < R] \\ &= P[SNR_{dB} < 10\log_{10}(2^{\frac{R}{B}} - 1)] \\ &= P[X_\sigma > TP - PL - P_{Noise} - 10\log_{10}(2^{\frac{R}{B}} - 1)] \\ &= P[X_\sigma > \beta_1] \end{aligned}$$

where $\beta_1 = TP - PL - P_{Noise} - 10\log_{10}(2^{\frac{R}{B}} - 1)$. As the probability follows Gaussian distribution, it is computed by

$$P[X_\sigma > \beta_1] = 1 - Q(\frac{\beta_1}{\sigma}) \tag{3.19}$$

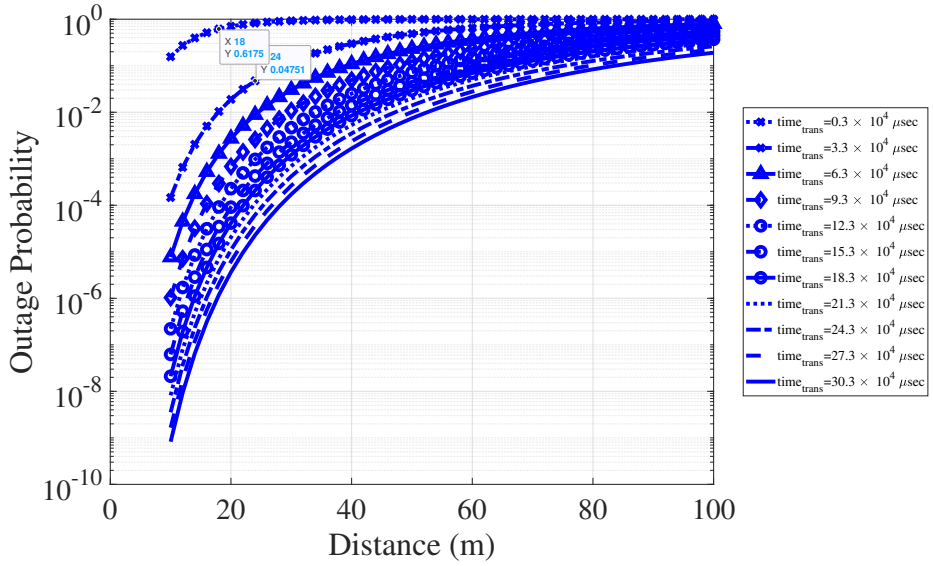


Figure 3.2: Outage probability versus the distance for various required transmission times

In Figure 3.2, the impact of various distances on the channel capacity is studied. As much as the distance increases, the outage probability decreases because of higher path-loss. In addition, the outage probability for the packets with high transmission time ($30.3 \times 10^4 \mu sec$) is better than the packets with low transmission time ($0.3 \times 10^4 \mu sec$).

Moreover, the impact of various required transmission time on the outage probability is measured as shown in Figure 3.3. The outage probability goes down when the distance and required transmission time increases.

In Figure 3.4, the outage probability versus noise signal (P_{Noise}) is examined for various distance values. The following remarks are concluded:

- as long as the noise signal P_{Noise} increases, the outage probability rises because it means that the noise signal is too high in-comparison with the received signal;
- a high distance results high probability of link outage which is close to 100%.

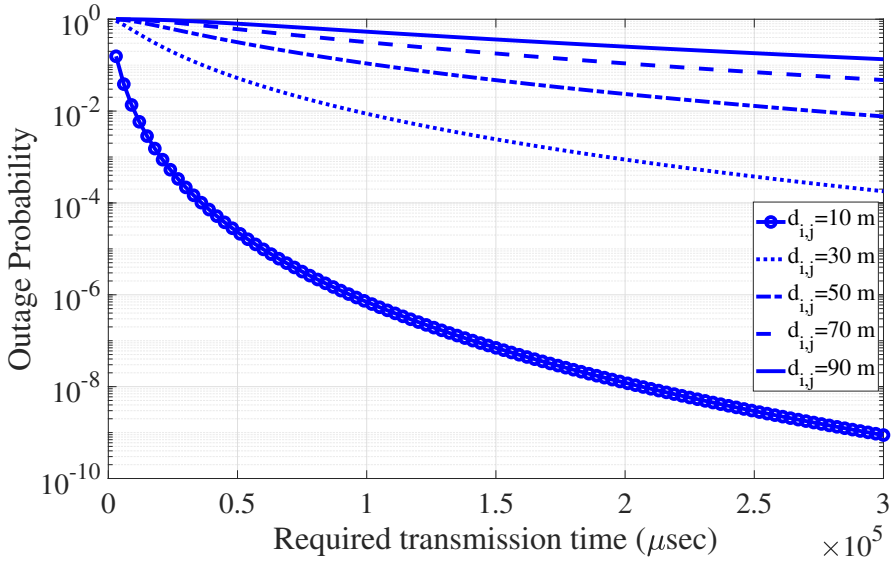


Figure 3.3: Outage probability versus required transmission times for various distance values

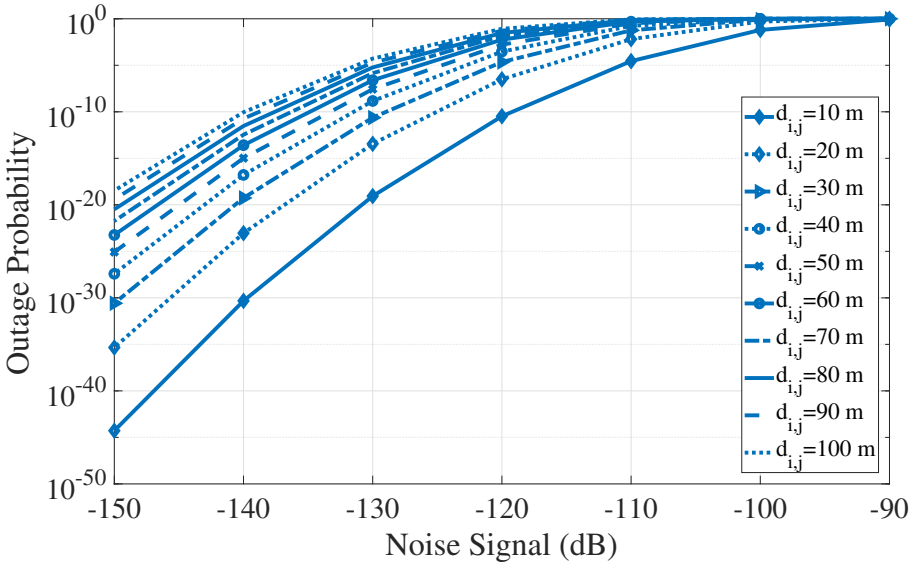


Figure 3.4: Outage probability versus noise signal (P_{Noise}) with various distance ranges

3.3.2 Outage Probability versus Transmission Power

Because some road entities have limited batteries, they may send the packet with low transmission power to save energy. As a consequence, the probabilities of link outage with various transmission power and distance are measured. The outage probability is computed by

$$\begin{aligned} P_{out}[RP < P_{th}] &= P[RP < P_{th}] \\ &= P[TP - PL - X_\sigma < P_{th}] \\ &= P[X_\sigma > TP - PL - P_{th}] \\ &= P[X_\sigma > \beta_2] \end{aligned}$$

where P_{th} is the power threshold and $\beta_2 = TP - PL - P_{th}$. The probability is expresses as Q-function as follows

$$P[X_\sigma > \beta_2] = Q(\frac{\beta_2}{\sigma}) \tag{3.20}$$

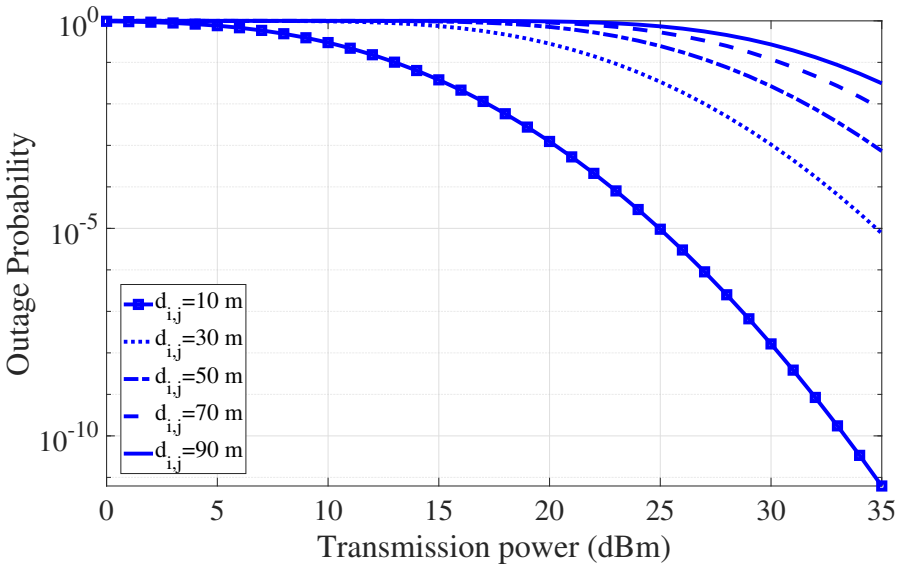


Figure 3.5: Outage probability versus transmission power and distance

The outage probability is required to determine the optimal distance for acceptable signal as shown in Figure 3.5. As the distance goes up, the outage probability increases as shown in Figure 3.5. When the distance between the sender and receiver is increased, the road entity requires to increase the transmission power to guarantee good signal.

3.3.3 Signal-to-Noise Ratio

Outage probability versus threshold SNR

In vehicular network, the signal could be affected by various obstacles such as large truck and buildings. Thus, the signal should have less noise when it is received. As a result, probabilities of link outage with various SNR thresholds and distance are computed. The outage probability

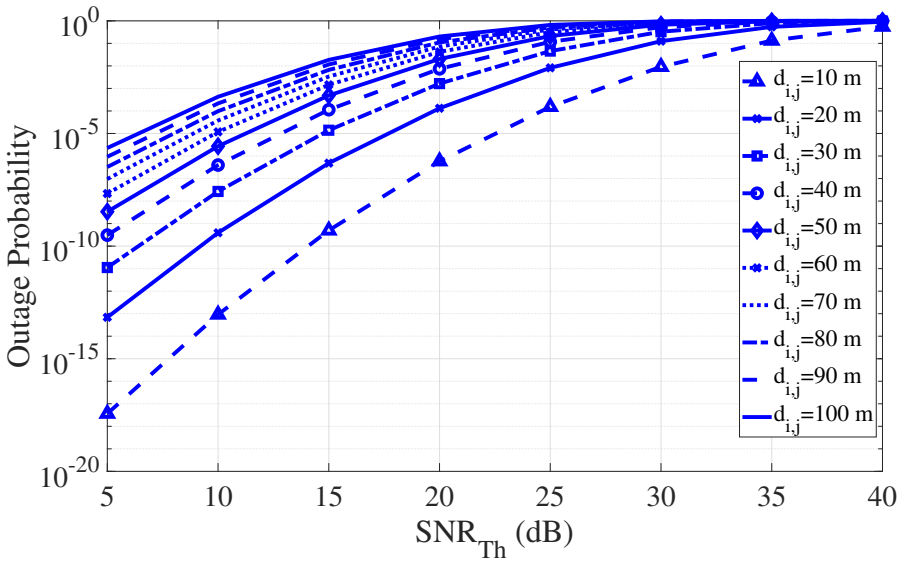


Figure 3.6: Outage probability versus threshold SNR (dB)

is given by

$$\begin{aligned} P_{out}[SNR_{dB} < SNR_{th}] &= P[SNR_{dB} < SNR_{th}] \\ &= P[TP - PL - X_\sigma - P_{Noise} < SNR_{th}] \\ &= P[X_\sigma > TP - PL - P_{Noise} - SNR_{th}] \\ &= P[X_\sigma > \beta_3]. \end{aligned}$$

where $\beta_3 = TP - PL - P_{Noise} - SNR_{th}$. When the distance between road entities is greater than 10 m as shown in Figure 3.6, low SNR thresholds are recommended to be able to achieve low outage probability.

3.4 Simulation Performance Analysis

A V2X network is considered with 100 road entities and 6 RSUs with parameters as shown in Table 3.3. The road entities move over an area of 800×800 m^2 with various speed ranges as

Table 3.3: Simulation parameters for studying the proposed algorithm

Parameter	Value
Simulation time (sec)	1000
Simulation area (m^2)	800×800
Number of nodes	100
Noise power (dBm)	-90
Bandwidth (MHz)	70
Frequency Band (MHz)	5855-5925
Packet size	510 Bytes
Data rate (R)	8.16 Mbps
Required transmission time (μsec)	500
Transmission Power (dBm)	23
Transmission Range (m)	250
Antenna height for UE - h_{UE} (m)	1.5
Average building height - h (m)	5
Queue capacity	25

Table 3.4: Mobility parameters

Road Entity	Speed range
Vehicle	[54-72] km/h
Motorcycle	[54-72] km/h
Cycle	[3.6-14.4] km/h
Pedestrian	[3.6-4.32] km/h

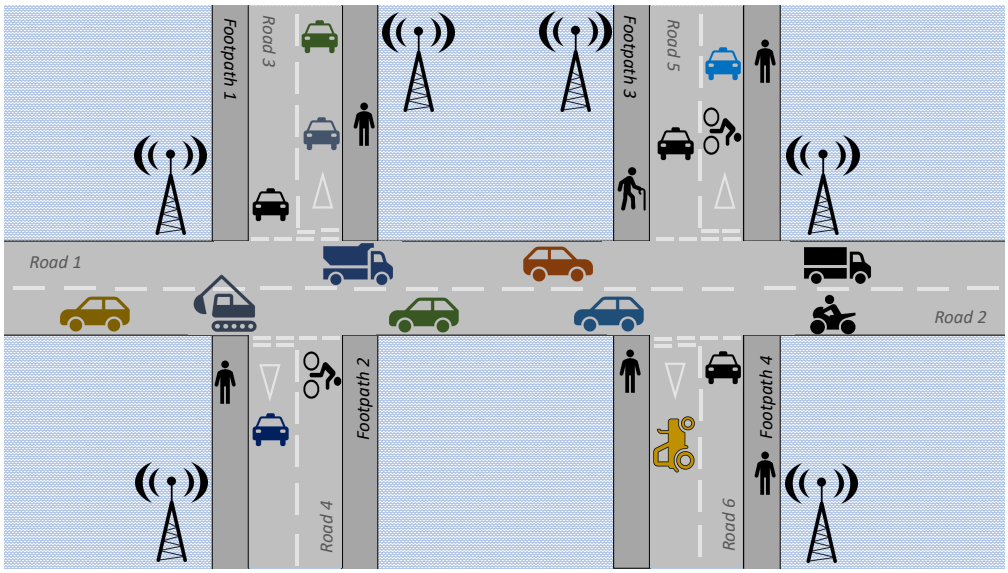


Figure 3.7: Simulation area in QoS-balancing relay selection algorithm

shown in Table 3.4. The road entity sends the transaction message to the core network directly or using a multi-hop routing protocol as shown in Figure 3.7. In addition, the considered network has heterogeneous nodes where the road entity includes vehicles, pedestrians, motorcycles and cycles.

3.4.1 Validation

To validate the simulation, the simulation results of the existing model are compared with the validated results [102] as shown in Figure 3.8. The simulation results are very close to the

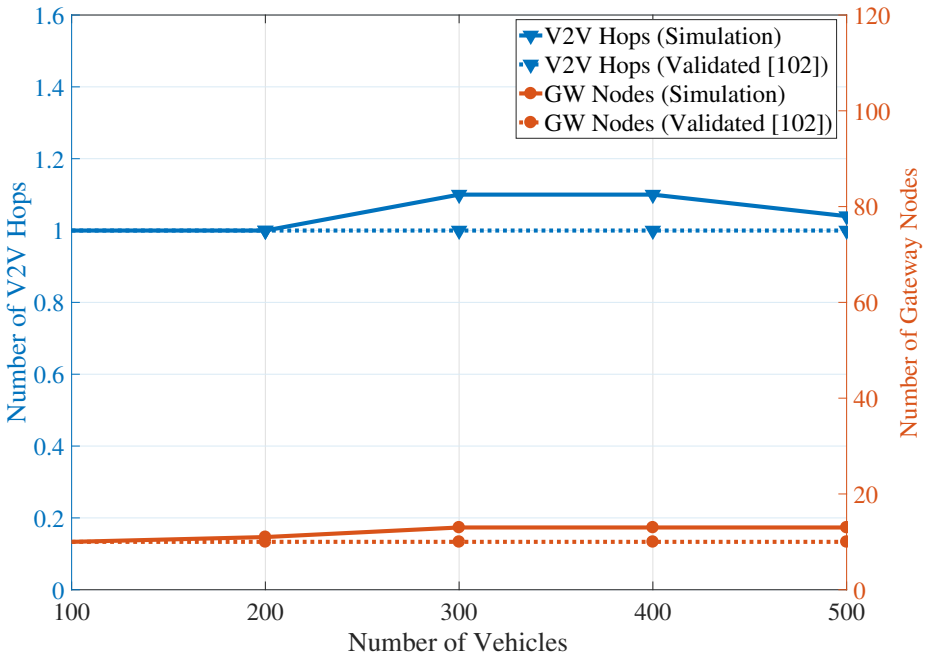


Figure 3.8: Validation results for average V2V hops and number of gateway nodes

validated one in both average V2V hops and the number of gateway nodes.

3.4.2 Existing Model Definition

The existing model [102] is used to evaluate the performance of the proposed model. Based on the literature review in Chapter 2, most of existing solutions were proposed to evaluate the link in vehicular network, however, they were applied on different communication protocol such as IEEE802.11p. Thus, this could cause a difference in link characteristics. As a result, this model is the one that evaluates LTE link in vehicular network which is very close to the proposed model. Here, both models are evaluated in two metrics which are PDR and end-to-end packet delivery ratio. The existing model suggested a hierarchical approach to decide if a vehicle should act as a gateway or not. In the first level of clustering, they proposed the fuzzy logic algorithm to choose

cluster heads. Then, they applied the Q-learning algorithm to choose some of cluster heads as gateways between IEEE802.11p and LTE networks.

Fuzzy logic algorithm

The competency value calculation consists of three steps. First, the velocity factor, leadership factor, and signal quality factor are calculated for each one-hop neighbor who is within the range of $\frac{1}{2}TR$ where TR is the transmission range.

Q-learning algorithm

They used a Q-learning algorithm to determine whether a cluster head should work as a gateway or not. The Q-value for a given action is determined by the discounted reward. If a vehicle is directly connected to the base station, the vehicle can get a positive reward. However, the value of the reward is decreased with the increase of the number of devices.

3.4.3 Measure the Complexity of the Proposed Algorithm

Here, the time complexity for the AHP algorithm. Each time the node would like to evaluate the link, it goes through the following calculations:

1. **Normalize (A) as shown in Eq(3.12):** In this case, the time complexity of computing the value is $n(n+1)/2$ which is equal to $O(n^2)$ where $n = 5$.
2. **Multiply the result of previous step by $\overrightarrow{ePCM}$:** This usual way to multiply a n×n matrix with a n×1 vector requires $(n \times n \times 1)$ multiplications and $n \times 1(n-1)$ additions, so asymptotically $2 \times n \times n \times 1$ elementary operations.
3. **Compute $\overrightarrow{ePCM}$ only once at the beginning:** Also, the computing of $\overrightarrow{ePCM}$ requires two nested for loops to measure the normalized value of PCM. Then, the time complexity is equal to: $O(n^2)$ where $n = 5$.

3.4.4 Experiment Results

The network throughput is evaluated by measuring two main metrics which are PDR and end-to-end packet delivery ratio. PDR is the rate of the packets that are generated but not delivered to the designated road entity. PDR evaluates the link between each two road entities. It is computed by

$$PDR_{i,j} = \frac{NI_{i,j}}{TI_{i,j}} \tag{3.21}$$

where $NI_{i,j}$ and $TI_{i,j}$ are the negative interactions and the total interactions between road entity i and road entity j, respectively. On the other hand, the end-to-end packet delivery ratio represents the percentage of the arrived packets to the core network. It is measured by

$$DR = \frac{AP}{GP} \tag{3.22}$$

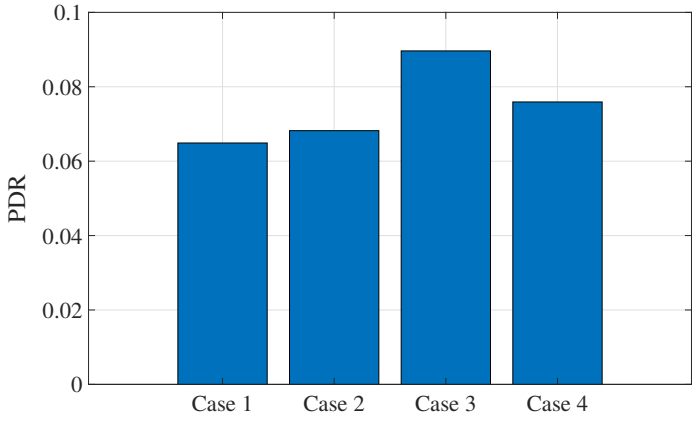
where GP is the total number of generated packets by all road entities, and AP is the number of arrived packets to the core network.

Investigating Different Metrics

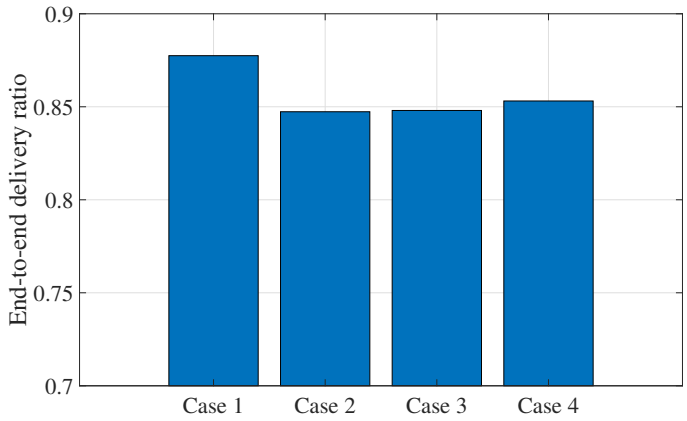
Here, the impact of various matrices on PDR and delivery ratio is studied. Various cases are assumed as follows:

- Case 1: Replace Channel capacity (C^t) with Direction (D^t.)
- Case 2: Replace Channel capacity (C^t) with Number of hops (H^t.)
- Case 3: Replace Channel capacity (C^t) with Acceleration (Acc^t.)
- Case 4: Replace Channel capacity (C^t) with Queue size (Q^t.)

In Figure 3.9 (a), case 1 ensures minimum value of PDR when the direction has the highest priority. On the other hand, the PDR is the highest in case 3 where the acceleration has a very low impact on the link. In addition, in Figure 3.9 (b), based on the previous result in (a, case 1 achieves the higher delivery ratio for the packets to the core network.



(a) PDR



(b) End-to-end delivery ratio

Figure 3.9: Investigating the impact of different metrics on: a) PDR; b) End-to-end delivery ratio

Evaluation measure for end-to-end delivery ratio

An experiment is conducted to study the performance of the proposed model in comparison with the existing model regarding the delivery ratio. As shown in Figure 3.10, the delivery ratio values are not stable and go up and down in both models. After time interval 300, the delivery ratio in the proposed model is approximately stable which means there is a balance between generation

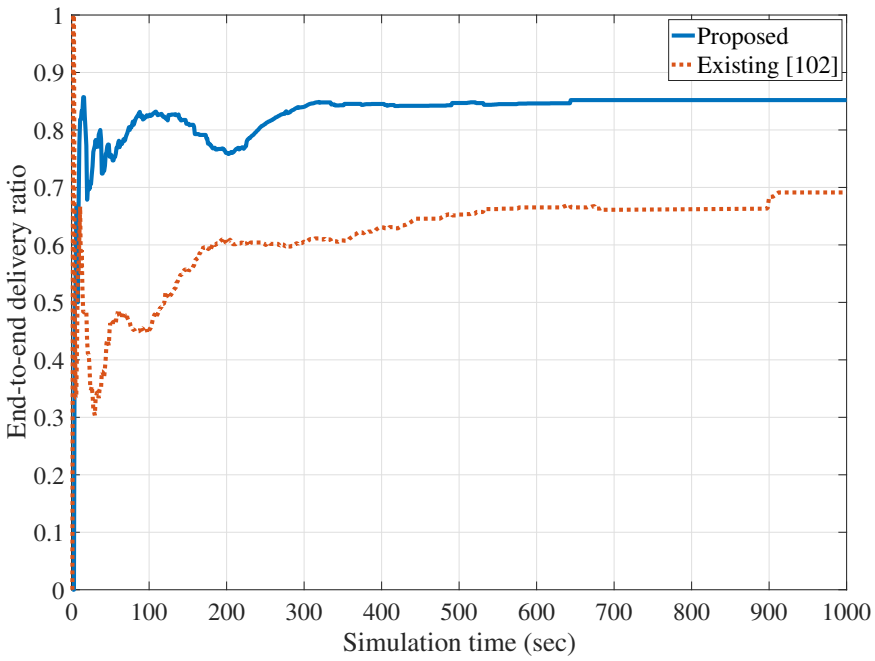


Figure 3.10: Evaluation measure for end-to-end delivery ratio during the simulation time

and arriving packets. On the other hand, it still goes up with time in the exiting model until it reaches 69%. This is means that the packets take more time to be delivered to the core network.

Evaluation measure for PDR

Another experiment is conducted to study the performance of the proposed model in comparison with the existing model regarding PDR as shown in Figure 3.11. The PDR starts with high values in the existing model then it goes down gradually with time. By the end of the simulation, the PDR is equal to 20% which is quite high because many surrounding nodes send their packets to the same gateway which causes congestion and buffer overflow at the gateway node. Thus, PDR value increases in the existing model. On the other hand, the PDR in the proposed model slightly decreases with time. In general, it has a stable curve during the simulation time. The proposed model achieves very low PDR in comparison with the existing model.

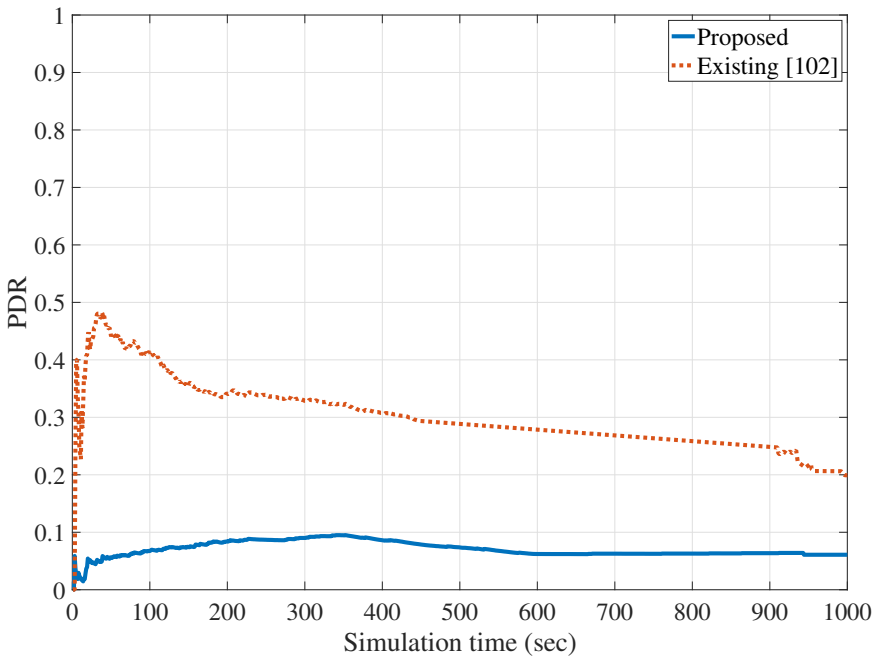


Figure 3.11: Evaluation measure for PDR during the simulation time

Impact of node density on delivery ratio and PDR

The impact of node density on end-to-end delivery ratio and PDR are studied. As shown in Figure 3.12, the delivery ratio increases when the number of road entity increases. This is because of the availability of various neighbors to deliver the packets to the core network. The proposed model achieves high delivery ratio which is around 90% when the number of road entities is equal to 250. On the other hand, the delivery ratio in the existing model starts with low value around 50% when the number of nodes is equal to 50. High number of road entities means that the road entity has broad choices to evaluate and choose the most stable link. In the proposed model, PDR is very low when the number of road entities exceeds 100 entities to reach to 3% when the number of road entities is equal to 250. However, the PDR in the existing model is quite high where it reaches 10% in the best case.

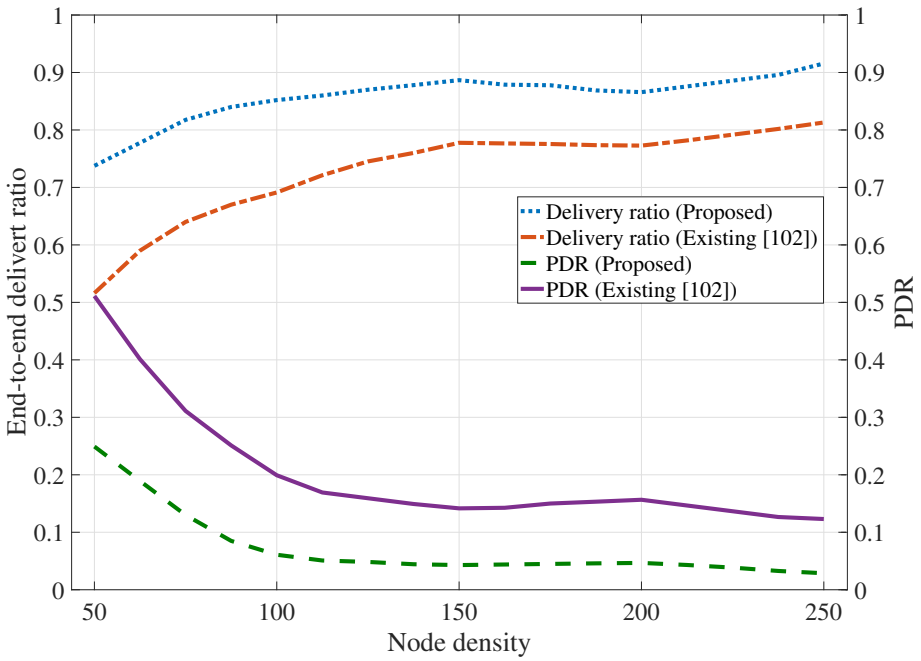


Figure 3.12: Impact of node density on end-to-end delivery ratio and PDR

Impact of road entity transmission range on delivery ratio and PDR

Various transmission ranges of road entity affects the detecting range of neighboring nodes (relaying nodes). Short range leads to less number of neighboring nodes. Thus, the road entity has few links to relay packets to the core network. In Figure 3.13, the impact of different transmission ranges on delivery ratio and PDR are studied. The ratio in the proposed model increases when the transmission range increases. On the other hand, the ratio in the existing model goes down because the range of electing cluster heads and gateways increases, thus, few number of cluster heads exist. In addition, the PDR in the proposed model is stable and not affected by the transmission range which achieves very low PDR that is equal to 5%. However, the PDR increases when the transmission range increases in the existing model because the large distance to the gateway gives higher outage probability. As a conclusion, the road entity in proposed model always chooses the trusted link and consider the distance to the relaying node.

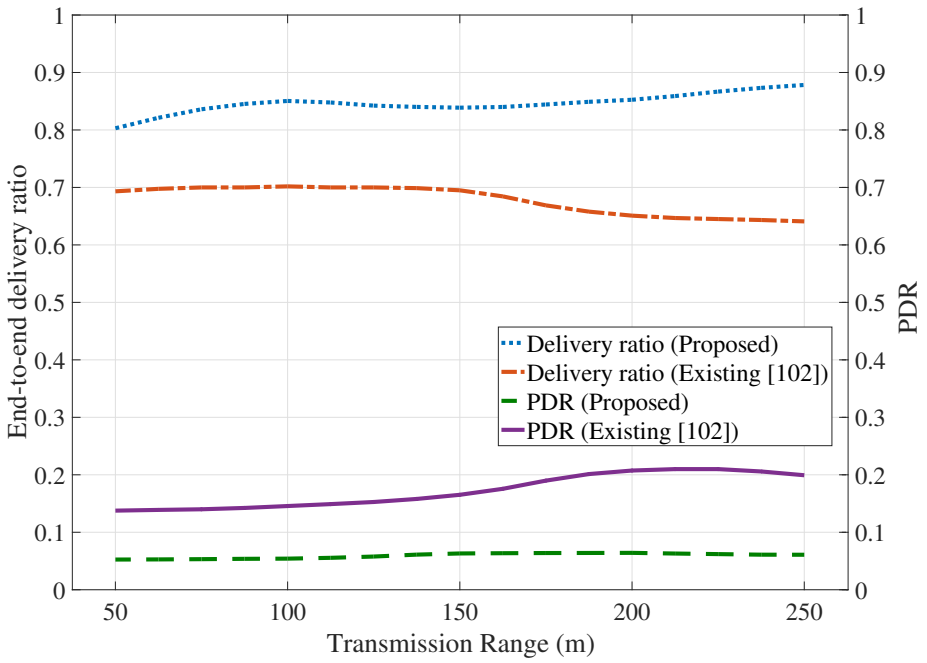


Figure 3.13: Impact of road entity transmission range on end-to-end delivery ratio and PDR

Impact of road entity speed on delivery ratio and PDR

The link outage, that is caused by node mobility, is the most challenge in vehicular network. As a consequence, the impact of road entity speed on the end-to-end delivery ratio and PDR are studied. As shown in Figure 3.14, the delivery ratio goes down when the entities' speeds increase in both models. However, the proposed model slightly decreases and achieves acceptable ratio of arrived packets to the core network, which is around 85% of total packets. The drop in delivery ratio in the existing model is higher than the proposed model which approximately reaches to 57%. On the other hand, the PDR increases when the speed increases in the existing model to reach 33% in the worst case. On the other hand, PDR in the proposed model slightly increases when the speed increases. As a result, the link stability in the proposed model is better than that in the existing model where the PDR is not highly affected by the road entity speed.

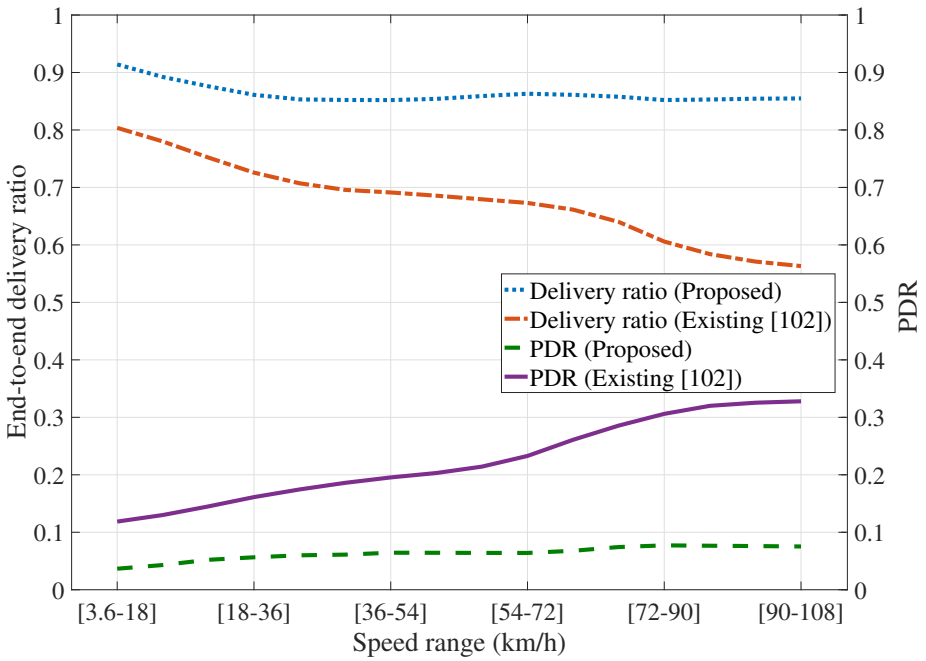


Figure 3.14: Impact of road entity speed on end-to-end delivery ratio and PDR

Study improvement rate

The improvement rate on delivery ratio and PDR for the proposed model in comparison with the existing model [102] is studied. Improvement rate of delivery ratio is computed by

$$Rate_{imp1} = \frac{|Value_{exist} - Value_{prop}|}{Value_{exist}} \tag{3.23}$$

where $Value_{prop}$ is the delivery ratio in the proposed model and $Value_{exist}$ is the delivery ratio in the existing model. Improvement rate of PDR is computed by

$$Rate_{imp2} = 1 - Rate_{imp1} \tag{3.24}$$

The improvement rate on the delivery ratio and PDR for various node densities are measured.

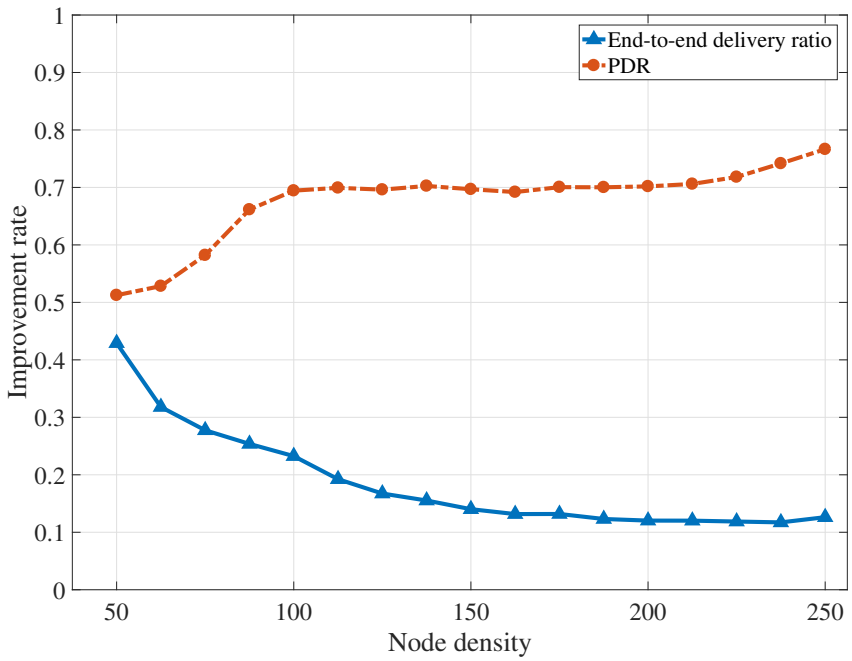


Figure 3.15: Improvement rate in the delivery ratio and PDR with various node densities

As shown in Figure 3.15, the delivery ratio starts with high improvement rate when the node density is equal to 50 because of the high difference between the values of proposed and existing models in Figure 3.12. As the node density goes up, the delivery ratio values for both models starts converging in Figure 3.12. Thus, the improvement rate for delivery ratio decreases. The proposed model improves the delivery ratio by 13% when the number of road entities equals 250. Also, the improvement in PDR decreases when the node density decreases. However, the PDR starts with higher improvement than the delivery ratio. At node density 250, the improvement in PDR reaches to 23%. As a conclusion, the behavior of the exiting model gets close to that of the proposed model when the node density increases.

Moreover, the improvement rate on delivery ratio and PDR for various node transmission ranges are evaluated as shown in Figure 3.16. The improvement in delivery ratio increases when the transmission range increases to reach 23%. It means that the proposed model is still able to

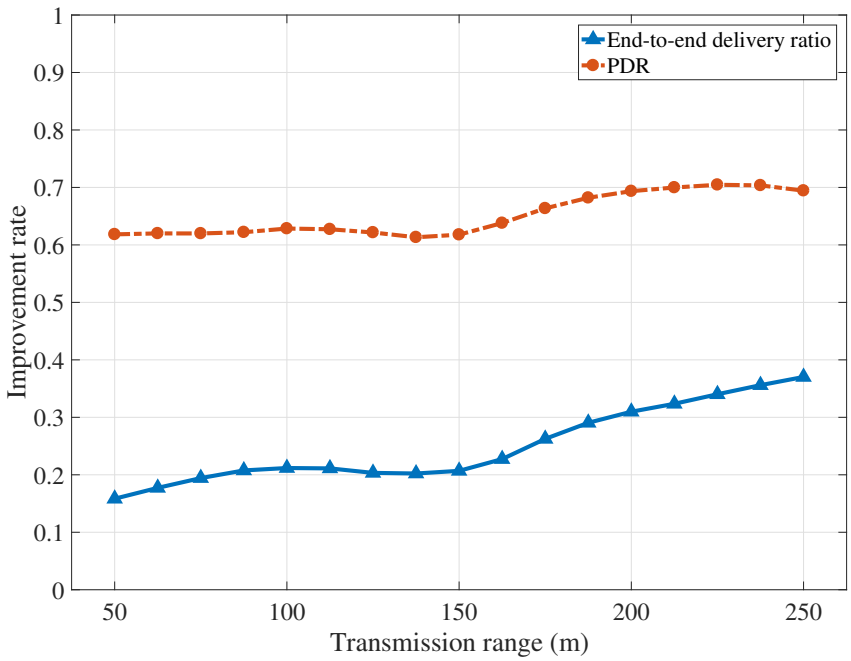


Figure 3.16: Improvement rate in the delivery ratio and PDR with various transmission ranges

choose the most stable link to deliver the packet with the increasing in distance between the source road entity and its neighboring entities. In addition, the improvement in PDR decreases when the transmission range increases. However, the improvement is less than the improvement in delivery ratio. Furthermore, the improvement rate on delivery ratio and PDR for various node speed are studied as shown in Figure 3.17. The improvement in the delivery ratio goes up when the road entity increases, however, the proposed model achieves low improvement rate on PDR when the speed increases. Thus, the proposed model achieves higher improvement in the delivery ratio in comparison with the PDR. Generally, the performance of the proposed model is able to ensure stable connection even with high mobility road entities.

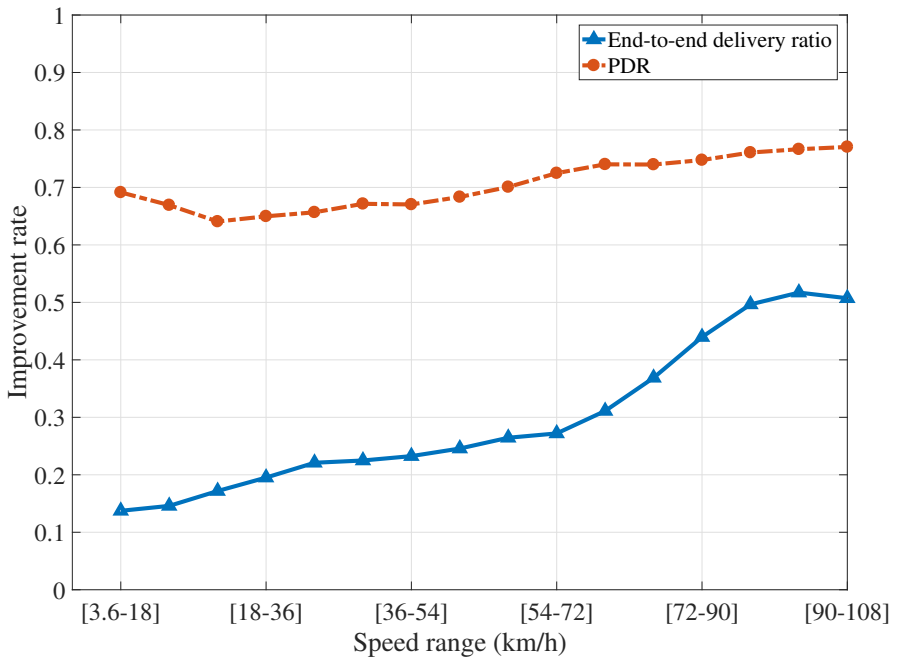


Figure 3.17: Improvement rate in the delivery ratio and PDR with various node speeds

3.5 Summary

In this chapter, a multi-metric QoS-balancing relay selection algorithm V2X communication was proposed. Various criteria were considered to evaluate the link quality, which are channel capacity, link stability, end-to-end delay. Also, the outage probability behavior was proposed based on the channel model in the LTE-A (release 14). The outage probability for various distances, transmission powers and SNRs were measured. Then, several experiments were conducted to evaluate the performance of the proposed model. The impact of various factors such as the number of road entities, the entity's transmission range and the entity's speed on PDR and delivery ratio were studied. The main conclusions are:

- The required transmission time for delay-sensitive messages is equal to 100 ms. Thus, the probability of having enough data rate is greater than 0.5 when the distance is less than

100 m.

- As long as the distance between road entities is less than $10m$, the probability of link outage is very low.
- When the road entity transmits the packets with a standard power of 23 dBm, the outage probability is less than 0.5 when the distance is around 50 m.
- The delivery ratio in the proposed model is stable most of the time, which means there is a balance between generating and arriving packets.
- Higher number of road entities leads to a higher number of potential links to relay the packets. Thus, the proposed model achieved very low PDR, which is equal to 3% when the number of road entities is 250.
- In the proposed model, a slight increase in delivery ratio was recorded when the transmission range increases because of the increasing of neighboring entities.
- In the existing model, the PDR increased when the speed increased to reach 33% in the worst case. On the other hand, PDR in the proposed model slightly increases when the speed increases where it is less than 10%.
- The simulation results showed that the proposed model improved PDR by 23% and delivery ratio by 13% in comparison with the existing model.

Chapter 4

Recommendation-based Trust Model for V2X Communication

Based on the literature review in Chapter 2, the detection of internal attacks is a common challenge in the vehicular network, especially non-stable malicious behavior as mentioned in Gap 1.1 in Chapter 1. Therefore, this chapter addresses this research gap and achieves Objective 2 in Chapter 1 by designing a trust-based model for V2X communications. In Chapter 3, the communication between road entities is improved by evaluating the link properties to choose the trusted communication link. However, the node behavior was not evaluated. Therefore, this chapter proposes a trust-based model to assess the entities' behavior. Thus, ensuring that the packet arrives using a trusted link (Chapter 3) to a trusted entity (Chapter 4).

Recently, some researchers designed trust models for vehicular networks to build up trust relationships among nodes [38, 53, 56, 62]. However, the node can only make a decision when there is a previous communication with the considered node. However, this is not the case in vehicular network where there is always high chance for meeting new nodes. To address new nodes

problem, recommendation-based trust model was suggested where the decision is based on direct interactions and the received recommendations. However, in some cases, the compromised node sends a fake recommendation regarding a normal node or other malicious node. As a result, adding recommendation filtering phase to the trust model was developed to ignore dishonest recommendations. For instance, some solutions in [121–124] suggested a recommendation-based trust model for choosing a trusted node. To overcome some of existing limitations such as centralized models and the existing of opinions, this chapter proposes a distributed recommendation-based trust model for protecting direct communications by excluding untrusted entities in the V2X network. The node can make a decision independently and detect malicious nodes prior to interactions. In addition, the proposed model is able to ignore the dishonest recommendations that are generated by highly trusted nodes. Furthermore, the impact of the non-stable malicious pattern is examined. Also, it presents a theoretical analysis and performance evaluation of the proposed model in comparison with the existing model [121].

4.1 Proposed System Model

A V2X communication technology is considered where it supports the connection between heterogeneous nodes in the vehicular network. This subsection explains the applied attacker model in details. In addition, it presents the main structure of the system model.

4.1.1 The Considered Network

We consider a vehicular network which consists of N road entities. The road entities include vehicles, pedestrians, cycles and motorcycles. Thus, they move at various speeds through a dedicated route. The communication in the considered network is provided by the LTE-V2X communication protocol. The side-link supports the direct connection between road entities. The nodes, which are located out of the network coverage, use relaying nodes to deliver their packets to the nearest eNB. Two types of nodes are considered as follows:

- *Normal node* which generates and sends its packets to the core network. Also, it relays any received packets towards the core network. In addition, the normal node keeps monitoring the surrounding nodes and evaluates their trustworthiness. If a misbehaving node is detected, the node blocks the communication with that node.

- *Malicious node* when a normal node is compromised and starts behaving maliciously. It aims to disturb the network and/or trust model performance. Generally, the nodes could use side-link to establish a multi-hop route to the nearest eNB. However, this is not working efficiently when the route has compromised nodes that launch the following internal attacks:

  - **Routing attacks** or denial-of-service attacks which affect the packet routing process by blocking the relayed packets such as blackhole attack where the compromised node drops all of the received packets; and greyhole attack where the compromised node discards some of the received packets selectively [21]. The impact of blackhole attack on the network performance is higher than greyhole attack. However, it is detected easily in comparison with greyhole attack.

  - **Recommendation attacks** which affect the decision phase in the trust model by sending fake recommendations regarding other nodes [125], as shown in Figure 4.1, such as good-mouthing attack where the malicious node f sends good recommendations regarding other malicious nodes $e_1, e_2, ... \ e_{np}$ as shown in Figure 4.1 (a). In this attack, the malicious nodes e could be considered as normal nodes. Thus, the malicious node f disturbs the decision phase; and bad-mouthing attack where the malicious node f sends bad recommendations regarding other normal nodes $q_1, q_2, ...$ q_{np} as shown in Figure 4.1 (b). In this attack, the normal nodes q may be classified by node i as malicious nodes. As much as the number of recommendation attackers rises, the negative impact on the trust decision increases. Thus, it becomes very hard for the normal nodes to make correct decisions regarding neighboring entities.

Moreover, the malicious node behavior follows various patterns which are *stable malicious behavior* where the malicious node behaves maliciously in a continuous manner and *non-stable*

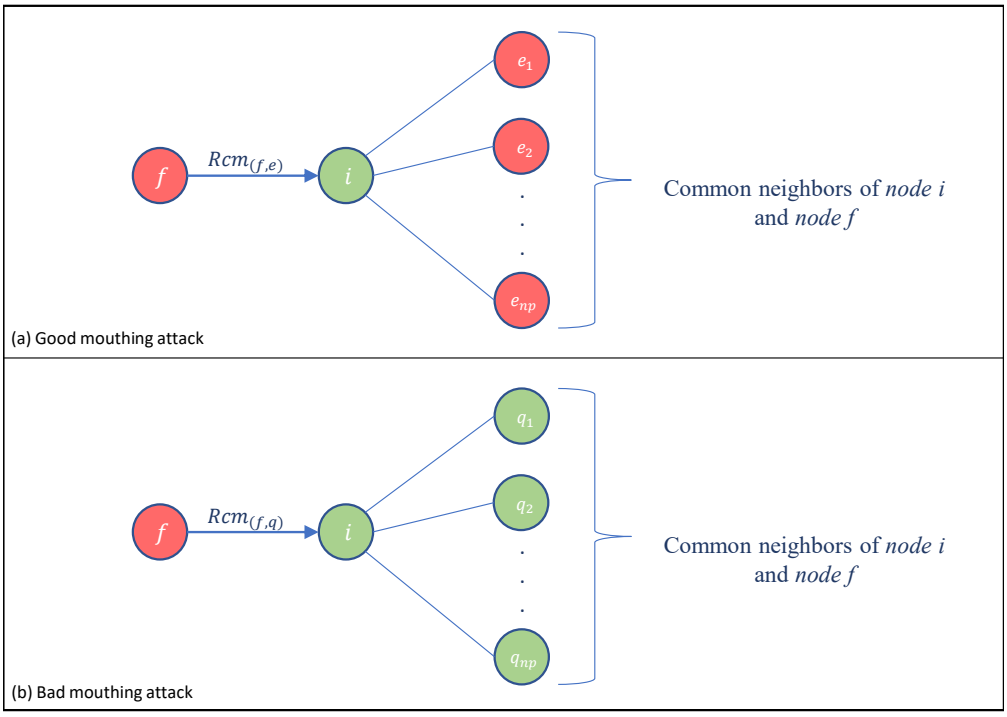


Figure 4.1: General model for recommendation attacks: a) Good-mouthing attack; b) Bad-mouthing attack

malicious behavior where the malicious node becomes smarter by behaving normally and maliciously in an alternative way. The malicious node behaves maliciously only with a specific neighbors or during intermittent time periods to keep itself undetected. Detecting this type of attackers is a challenge because in a short time they can gain high trust values [126].

4.1.2 System Model

Each time the road entity has information to send to the core network, it should go through four phases as follows:

- *Network coverage phase:* Each road entity continuously checks its connectivity with the core network and neighboring nodes. If it is located in-network coverage, it specifies the

nearest RSU or eNB to communicate with. Otherwise, it looks up for a nearby entity to relay its packets.

- *Communication phase:* If the road entity has a direct link with eNB, it sends the packet directly through the network. Otherwise, the source entity i measures the trustworthiness degree for the relaying entity j. If road entity j is trusted, the entity i sends the packets to road entity j. Otherwise, it searches for another neighboring entity. In case there is no trusted neighboring entities, it should wait till a connection with the network or trusted entity is established.

- *Trust calculation phase:* Trust calculations are executed on the road entity level in a distributed manner. Each road entity is able to compute trust value for surrounding entities. This phase maintains two levels of trust: direct and indirect. This phase is explained in details in Subsection 4.2.

- *Decision phase:* Each road entity has a local blacklist where the malicious neighboring entities are added to its blacklist. Decision is made based on total trust value as shown in Subsection 4.2.

4.2 Recommendation-based Trust Model for V2X

The proposed model is designed to protect V2X communication against internal attacks. The direct communication with surrounding road entities creates a trust relationship. It is measured as a continuous valued variable in the range of $[0, 1]$, in which 0 means that the node is untrustworthy and 1 means that the node is trustworthy. Trust relationship could be improved or broken based on positive and negative interactions with the surrounding entities. In addition, the other entities' opinion affect on some ways on the trust relationship. However, these recommendations should be filtered to discard any dishonest recommendations. Therefore, the road entity becomes able to make accurate decisions regarding the neighboring entities. Building on a comprehensive review in [4], the summary offered that the weighted sum and fuzzy logic are the most common methods to measure trustiness in vehicular networks. Furthermore, in previous work [127], a comparison

between the trust methods for the vehicular network scenario was proposed. These results showed that the weighted-sum is more efficient than fuzzy logic. Therefore, trust calculations in the proposed model are executed in a distributed manner using weighted-sum method. The trust calculation includes two main trust components as follows:

4.2.1 Current Trust - $T^{(t)}_{c(i,j)}$

It is an evaluation of the current relationship between node i and node j during the time interval t. The evaluation is measured based on the current and past experience with node j. It is computed by

$$T^{(t)}_{c(i,j)} = \frac{T^{(t)}_{p(i,j)} + T^{(t)}_{d(i,j)}}{2} \tag{4.1}$$

where $T^{(t)}_{p(i,j)}$ is the past trust measure of node i regarding node j, and $T^{(t)}_{d(i,j)}$ is the direct trust value between node i and node j. Because of the importance of both past and direct trust, the same weight is given for them. Here is the detailed description:

Past trust - $T^{(t)}_{p(i,j)}$

It is a measure of the historical behavior of each node j. The node i records the last computed total trust value for the node j which it has previous communications with them. In case of node i does not have previous communication with node j, the past trust value will be equal to the initial trust value $T^{(0)}_{t(i,j)}$. In addition, the smart attacker could stop behaving maliciously for a long time. Therefore, it behaves normally in current period, however, its past trust value is very low which assists neighboring nodes to detect the attacker correctly. It is calculated as

$$T^{(t)}_{p(i,j)} = T^{(t-\Delta)}_{t(i,j)} \tag{4.2}$$

where Δ is the time for the last computed trust value of node j, and $T_{t(i,j)}$ is the latest total trust value during time interval $(t - \Delta)$. Because the topology in vehicular network frequently changes, node i meets different nodes each time interval t. Therefore, Δ value is not fixed and varies based on the last communication with node j.

Direct trust - $T^{(t)}_{d(i,j)}$

Each road entity monitors surrounding entities for packet forwarding service. Node i computes the direct trust of its one-hop neighboring node j which is based on the direct interactions between them. Thus, it is calculated only when there is a direct communication between node i and node j at time t. During the interaction, node i collects information regarding the sent packets and whether node j relayed them or not. Therefore, it uses the collected information to compute the direct trust value which represents the forwarding packet rate during the time interval t. It is calculated using

$$T^{(t)}_{d(i,j)} = \frac{SI_{(i,j)}}{TI_{(i,j)}} \tag{4.3}$$

where $SI_{(i,j)}$ is the successful interactions between node i and node j, and $TI_{(i,j)}$ is the total interactions between node i and node j. As much as the forwarding rate increases, the direct relationship gets improved. The direct trust has the same importance as the past trust. For instance, the normal node could be compromised and starts behaving maliciously, however, its past behavior is trusted. Thus, the low direct trust value helps surrounding entities to detect the compromised nodes.

4.2.2 Indirect Trust - $T^{(t)}_{in(i,j)}$

It is a measure for trust relationship depending on the surrounding nodes' opinion. Consequently, node i sends requests to the neighboring nodes k to collect their recommendations regarding node j. Indirect trust is a distributed operation where all nodes can compute indirect trust based on the received recommendations at time t. To achieve an accurate result, the recommender node k should only send its recommendation about node j if it had a previous communication with it. The following steps are proposed to filter out the dishonest recommendations:

Confidence value - $C^{(t)}_{(i,k)}$

The confidence value measures to which extent the node i can trust the recommender node k. Thus, the node i computes the confidence value for each recommender node k depending on the

Input: $Th_T, Th_C, L \leftarrow$ list of node i neighbors which have a previous direct communication with node j
Output: $T^{(t)}_{in(i,j)}$

$P^{(t)}_{(i,j)} \leftarrow 0$
$a \leftarrow 0$
for each node L(k) **do**
  if $T^{(t)}_{t(i,L(k))} \geq Th_C$ **then**
    $C^{(t)}_{(i,L(k))} \leftarrow 1$
  else
    if $T^{(t)}_{t(i,L(k))} \geq Th_T$ **then**
      $C^{(t)}_{(i,L(k))} \leftarrow 0.8$
    else
      $C^{(t)}_{(i,L(k))} \leftarrow 0$
    end if
  end if
  $P^{(t)}_{(i,j)} \leftarrow P^{(t)}_{(i,j)} + (C^{(t)}_{(i,L(k))} \times T^{(t)}_{t(L(k),j)})$
  $a \leftarrow a + 1$
end for
$T^{(t)}_{in(i,j)} \leftarrow \frac{P^{(t)}_{(i,j)}}{a}$

Algorithm 4.1: Algorithm for computing indirect trust

total trust value $T^{(t)}_{t(i,k)}$. The confidence value is computed by

$$C^{(t)}_{(i,k)} = \begin{cases} 1, & \text{if } T^{(t)}_{t(i,k)} \geq Th_C \\ 0.8, & \text{if } Th_T \leq T^{(t)}_{t(i,k)} < Th_C \\ 0, & \text{if } T^{(t)}_{t(i,k)} < Th_T \end{cases} \tag{4.4}$$

where Th_C is the confidence threshold, and Th_T is the trust threshold. Based on (4.4), the normal node has 80% confidence level when its trust value is between the confidence threshold and the trust threshold. As much as the trust value increases and exceeds the confidence threshold, the recommender node is fully trusted. In addition, the recommendations which are sent by malicious nodes are ignored.

Indirect trust measure

The indirect trust value is measured as an average value of the received recommendations regarding node j. Therefore, node i calculates the indirect trust for node j using

$$T_{in(i,j)}^{(t)} = \frac{\sum_{k=1}^{a}[C_{(i,k)}^{(t)} \times T_{t(k,j)}^{(t)}]}{a} \tag{4.5}$$

where a is the total number of recommendations. The indirect trust computation works as shown in Algorithm 4.1.

4.2.3 Total Trust - $T_{t(i,j)}^{(t)}$

Each node is able to make a decision regarding nearby nodes by computing total trust value. Because the vehicular network has a dynamic topology, the node experiences various communication cases. Therefore, not all trust components are computed each time and for all cases. For example, in case of traffic jamming in the city center, the topology is stable for a period of time. Thus, the past trust should be considered. As a consequence, node i examines three parameters before calculating the total trust value for node j as follows:

- New communication: which determines whether the connection between node i and node j is for the first time.
- Existing of recommendations: which checks whether node i has common neighbors with node j and they have recommendations regarding node j.
- Current communication: which determines if there is a communication between node i and node j during the current interval.

The evaluation of the total trust can be done using Figure 4.2, where all possible scenarios in V2X communications are considered as follows:

- *Case 1: There is no current communication <u>BUT</u> there are recommendations.*

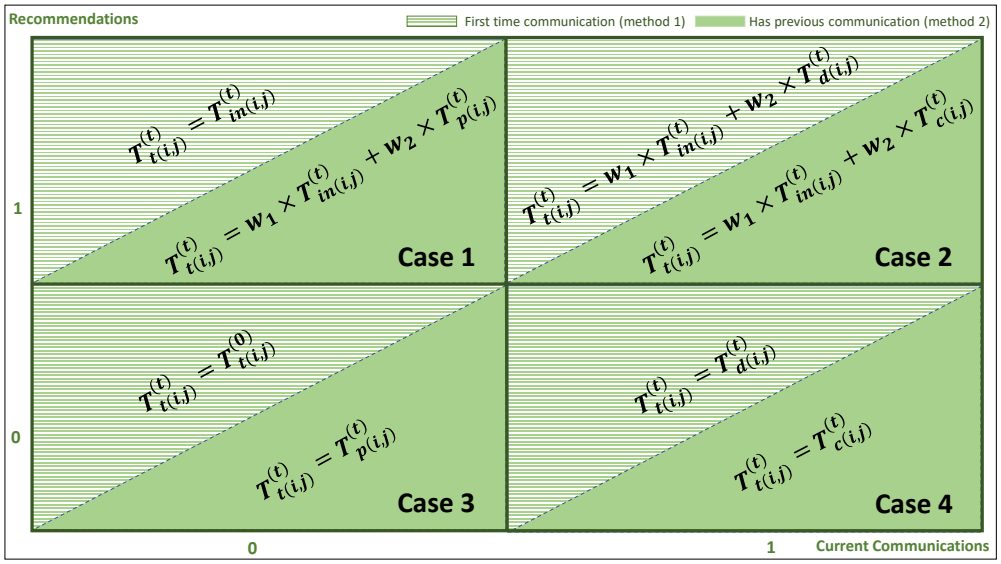


Figure 4.2: Total trust decision mapping in the proposed model

- *Case 2: There are current communications AND recommendations.*
- *Case 3: There is no current communication AND no recommendations.*
- *Case 4: There are current communications BUT no recommendations.*

Depending on whether previous communications exist, the total trust is updated using two different methods:

Method 1

When node i establishes the communication with node j for the first time. In this scenario, the current trust is ignored because node i does not have an accurate past trust value for node j.

Thus, the direct and indirect trust are only considered. Total trust is measured by

$$T_{t(i,j)}^{(t)} = \begin{cases} T_{in(i,j)}^{(t)}, & \text{Case 1.} \\ w_1 \times T_{in(i,j)}^{(t)} + w_2 \times T_{d(i,j)}^{(t)}, & \text{Case 2.} \\ T_{t(i,j)}^{(0)}, & \text{Case 3.} \\ T_{d(i,j)}^{(t)}, & \text{Case 4.} \end{cases} \tag{4.6}$$

In case 1, the indirect trust is only counted because node i only has recommendations regarding node j. Whereas, when the current communication exists in case 2, node i evaluates node j based on a weight-sum of direct and indirect trust. In case 3, node i does not have any information about node j. Thus, the initial total trust value is used. Finally, the direct trust is only evaluated in case 4 because of lacking enough recommendations about node j.

Method 2

When node i has previous communications with node j. Thus, node i has an updated value for past trust of node j. In this scenario, the current trust is measured when direct trust has a value. Otherwise, the past trust and indirect trust are only counted. Total trust is computed using

$$T_{t(i,j)}^{(t)} = \begin{cases} w_1 \times T_{in(i,j)}^{(t)} + w_2 \times T_{p(i,j)}^{(t)}, & \text{Case 1.} \\ w_1 \times T_{in(i,j)}^{(t)} + w_2 \times T_{c(i,j)}^{(t)}, & \text{Case 2.} \\ T_{p(i,j)}^{(t)}, & \text{Case 3.} \\ T_{c(i,j)}^{(t)}, & \text{Case 4.} \end{cases} \tag{4.7}$$

where w_1 and w_2 are weights for indirect trust and (direct/current or past) trust, respectively. w_1 represents the recommendation rate as follows:

$$w_1 = a \times \frac{RC}{Neighbors^{(t)}} \tag{4.8}$$

where $Neighbors^{(t)}$ is the number of node i neighbors at time t, RC is the recommendation factor, $a \leq Neighbors^{(t)}$, and $w_2 = 1 - w_1$.

Because there are recommendations regarding node j in case 1, node i is able to compute a weighted-sum of indirect and past trust. On the other hand, when the current communication is established in case 2, node i can measure current trust and indirect trust. In case 3, node i can only compute past trust value of node j. Current trust is only considered in case 4 when there are no recommendations regarding node j.

Moreover, each node computes the total trust for all neighboring nodes. The time complexity for computing direct trust value is equal to $O(1)$ as Eq(4.3) is a linear equation. But because it is computed for each neighbor, the complexity becomes equal to $O(Neighbors^{(t)})$. Then, the node starts collecting recommendations for regarding the neighboring nodes. The time complexity for computing indirect trust is equal to $O(Neighbors^{(t)} \times a)$ where $Neighbors^{(t)}$ is the number of neighboring nodes and a is the total number of recommendations about node j. Finally, the time complexity for computing the total trust value for each neighboring nodes is equal to $O(Neighbors^{(t)})$.

4.2.4 Trust Decision

Based on the calculated total trust value, the node is able to make local decisions regarding the surrounding nodes. Every node has a local blacklist which contains a list of untrusted nodes based on its decision. Thus, node i blocks the communication with any node j in the blacklist. Based on a predefined trust threshold (Th_T), the decision is made by

$$Decision = \begin{cases} Trusted, & \text{if } T^{(t)}_{t(i,j)} \geq Th_T. \\ Untrusted, & \text{if } T^{(t)}_{t(i,j)} < Th_T. \end{cases} \tag{4.9}$$

4.3 Simulation Analysis

Here, the simulation set-up is presented to study the performance of the proposed model. Also, the mobility parameters for various road entities are suggested. In addition, various experiments with various malicious behaviors are conducted.

4.3.1 Network Specifications

A V2X network is considered with 24 road entities and two RSUs with parameters as shown in Table 4.1. Trust threshold value (Th_T) is chosen in the middle of trust value range because once the threshold goes above 0.5, the False Positive Rate (FPR) value increases. Also, the False Negative Rate (FNR) value increases when the threshold becomes less than 0.5. Therefore, the initial trust value $T^0_{t(i,j)}$ is equal to 0.5 to be very sensitive for any malicious behavior. As shown in Figure 4.3, the road entities move over an area of 800×800 m^2 with various speed ranges. The proposed communication scenario is related to direct links in cellular networks. The road entity only uses the multi-hop route when it is located out of the network coverage. Therefore, computing trust value for the neighboring nodes in this scenario is a challenge because the node does not continuously communicate with the neighboring nodes. In addition, the considered network has heterogeneous nodes where the road entity is not limited to vehicles but also includes pedestrian, motorcycles and cycles with various speeds as shown in Table 3.4 in Chapter 3.

Table 4.1: Simulation parameters for studying the performance of recommendation-based trust model

Parameter	Value
Simulation time	80 iterations
Simulation area (m^2)	800×800
Number of nodes	24
Th_T	0.5
Th_C	0.8
$T^{(0)}_{t(i,j)}$	0.5
RC	0.5

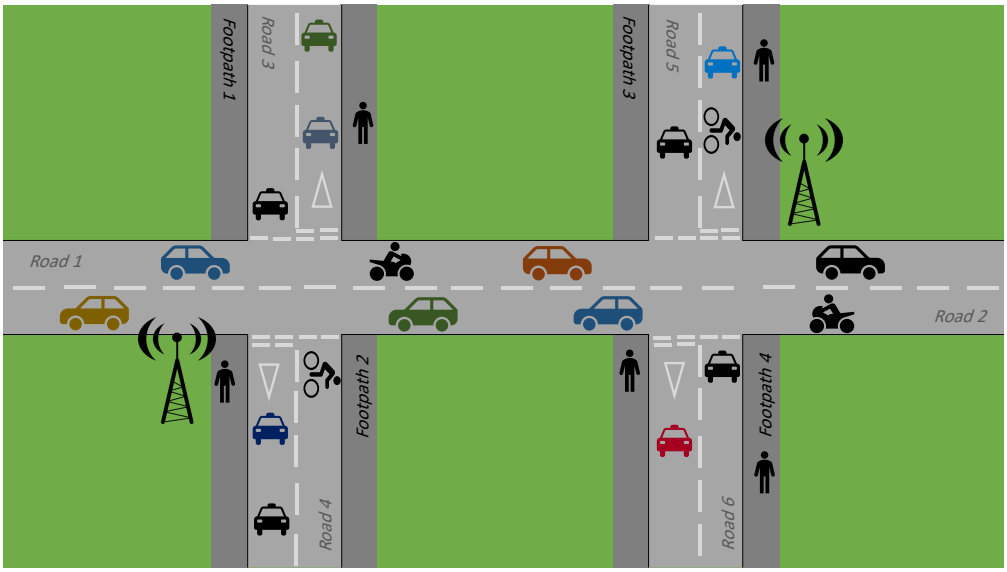


Figure 4.3: Simulation area in recommendation-based trust model

Thus, the connection time could vary depending on the speed of source and destination nodes. To measure the performance of the proposed trust model, four malicious behaviors are studied which are blackhole attack, greyhole attack, bad-mouthing attack and good-mouthing attack.

4.3.2 Evaluation of Fuzzy Logic Algorithm in Decision Making

Various behavior-based solutions were proposed for addressing the internal attacks. Based on the literature review in Chapter 2, the most common methods are: weighted-sum and fuzzy logic. The proposed model applied weighted-sum in total trust calculations. The decision of using this method is based on a comparison between various trust-based methods in a previous work [127]. Fuzzy logic algorithm incorporates a series of IF-THEN rules to solve a control problem rather than attempt to model a system mathematically. The main steps of the fuzzy logic model are as follows [61]. *First*, the fuzzy sets and criteria are defined; *next*, the input variable values are initialized; *then*, the fuzzy engine applies the fuzzy rules to determine the output data and evaluate the results. To evaluate fuzzy logic method, the weighted-sum equations in Figure 4.2 are replaced by fuzzy logic as shown in Figure 4.4 where the linguistic inputs are indirect trust and

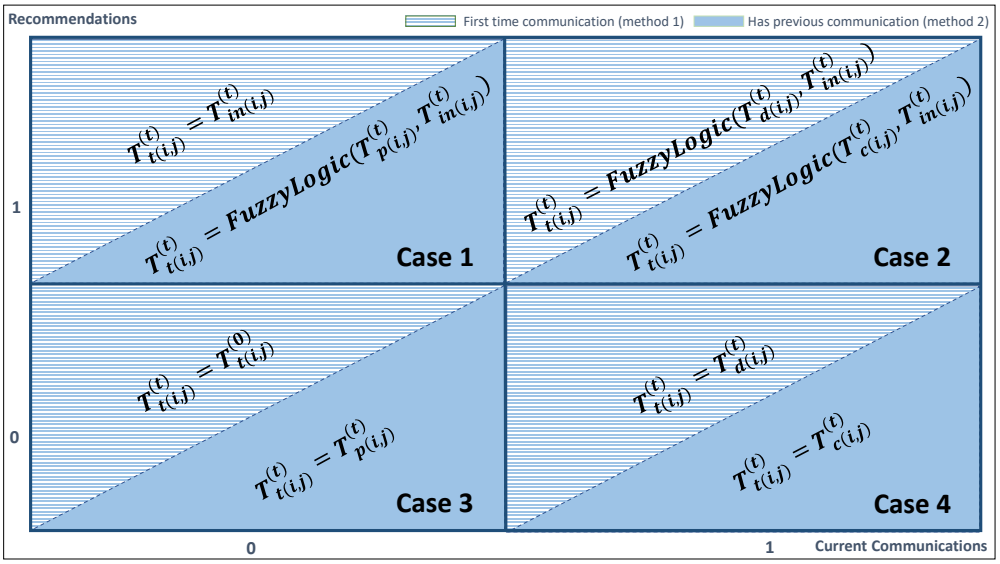


Figure 4.4: Total trust decision mapping with fuzzy logic algorithm

(past/current/direct) trust as shown in Figure 4.5. The input linguistic variables are connected through AND logical operator. The membership functions were used are proposed in [126] and shown in Figure 4.6. Then, trust values are calculated by passing the fuzzy sets described in [126] through fuzzy inference rules. Total trust ($T^{(t)}_{t(i,j)}$) uses Triangular and Trapezoidal Membership

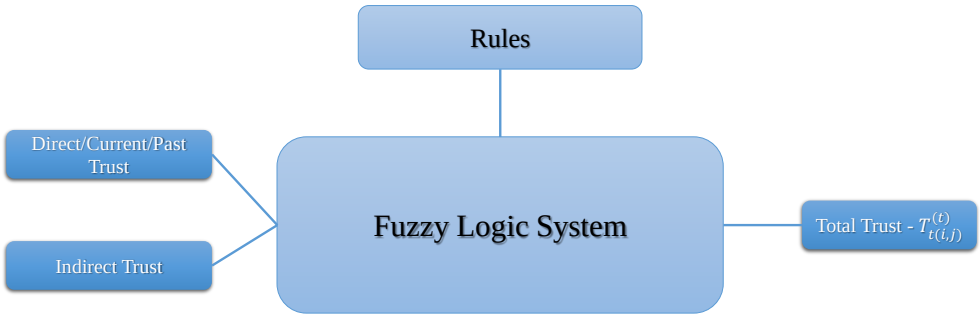
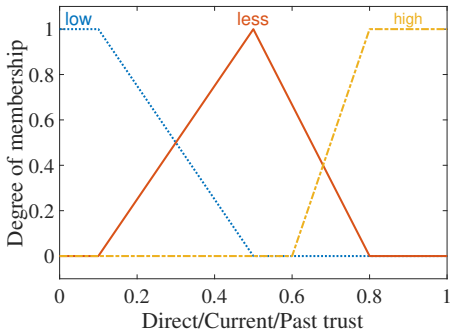
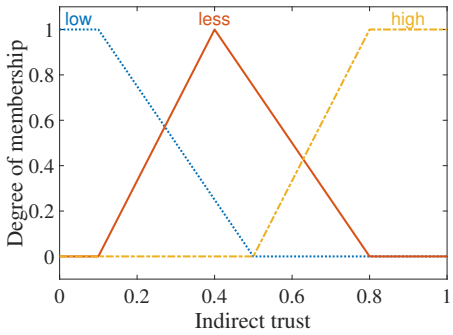


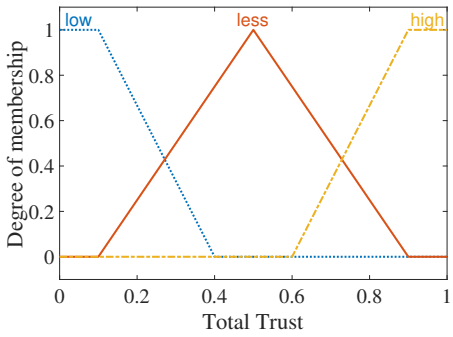
Figure 4.5: Fuzzy logic system structure in [126]



(a) Direct/Current/Past trust



(b) Indirect trust



(c) Total trust

Figure 4.6: Fuzzy membership function for decision variables: (a) Direct/Current/Past trust; (b) Indirect trust; (c) Total trust

Functions which are specified by three parameters: Malicious, Less Trusted, and Normal. The number of the input linguistic variables is two in the proposed method and each variable takes

Table 4.2: Fuzzy if-then control rules

Rule Num	Direct/Current/Past trust	Indirect trust	Total trust
1	Low	Low	Low
2	Low	Less	Low
3	Low	High	Less
4	Less	Low	Low
5	Less	Less	Less
6	Less	High	Less
7	High	Low	Less
8	High	Less	High
9	High	High	High

three values. Thus, the total number of rules, with all possible combinations, is 9 as shown in Table 4.2. After fuzzification, the next step is a defuzzification to get crisp values using mathematical method.

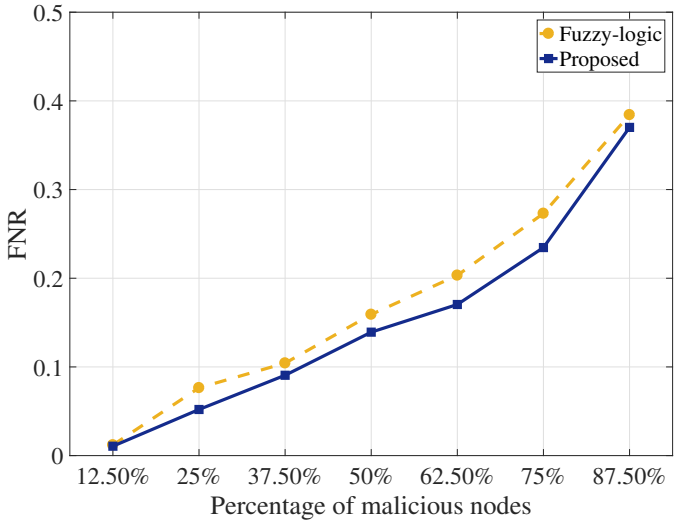
Comparison results

FNR is evaluated with various percentage of malicious nodes in Figure 4.7 (a). As much as the percentage of malicious nodes increases, the FNR values go up for both methods. FNR in fuzzy logic starts with same value as weighted-sum when the percentage is equal to 12.50%. However, FNR in weighted-sum achieves lower rate than fuzzy logic.

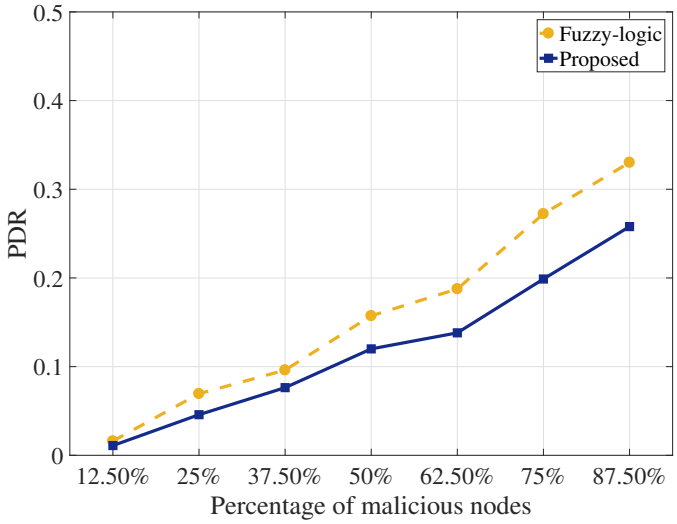
Moreover, PDR is measured with various percentage of malicious nodes in Figure 4.7 (b). The PDR values start with approximately same values which are equal to 0.01. As much as the percentage of malicious nodes increases, the difference between the PDR of both methods increases. When the percentage of malicious nodes is equal to 87.50%, the PDR equals 0.33 in the fuzzy logic method.

4.3.3 Study the Performance of the Proposed Model

In this subsection, the network performance is studied by measuring PDR and network throughput in the existence of blackhole and greyhole attacks. In addition, the impact of various attacks



(a) FNR



(b) PDR

Figure 4.7: Comparison results for various decision making algorithms: a) FNR; b) PDR

on the total trust value is studied.

Network Performance

The performance of the entire network is represented by two parameters, which are PDR and network throughput, in the presence of malicious nodes. PDR is calculated using (3.22). The network throughput is measured by the percentage of packets that are sent successfully. It is calculated using

$$Network\_Throughput = \frac{SP}{TP} \tag{4.10}$$

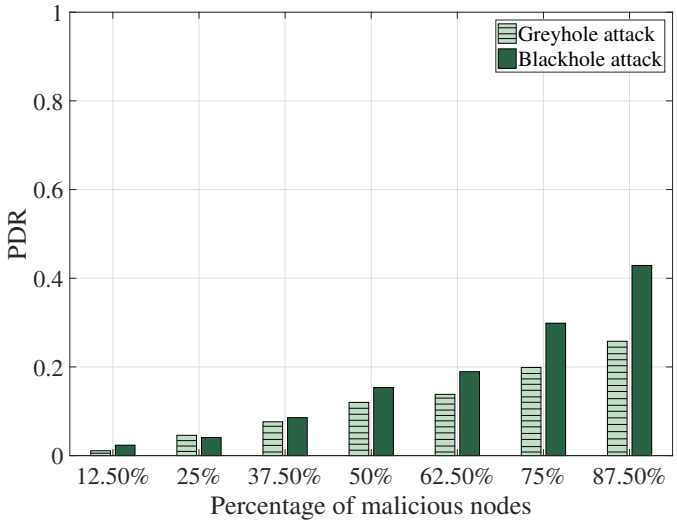
where SP is the number of packets that are successfully sent and TP is the total number of generated packets in the network.

In Figure 4.8 (a), the PDR keeps increasing until reach approximately 0.4 in the worst case when the percentage of malicious nodes is more than or equal to 87.50% and all malicious nodes are blackhole attackers. On the other hand, in the greyhole attack, the dropping rate also increases but with a lower rate.

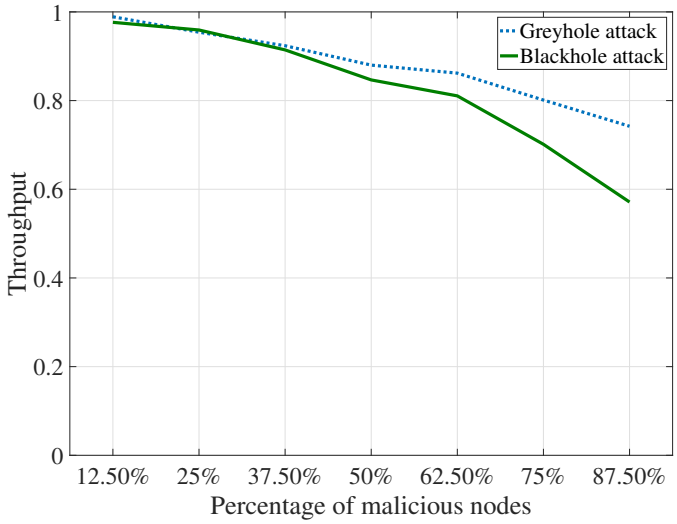
Moreover, the network throughput is measured as shown in Figure 4.8 (b). In case of greyhole attack, the proposed model can keep the value of throughput greater than 0.7 even in case of the high percentage of malicious nodes. While in the blackhole attack, the network performance decreases to reach 0.65 in the worst case.

Detection Rate for Blackhole/Greyhole attackers

Blackhole attack is easier to detect than greyhole attack because the malicious node in the blackhole attack drops all of the received packets. In Figure 4.9, the trust value starts with the initial value which is equal to 0.5. In blackhole attack, at the first intervals when the malicious behavior is launched, the trust value drops to 0.08 which is a small value; then, the trust value gradually decreases with time. In the greyhole attack, during the first intervals, trust value increases because of a low dropping rate; then, trust value goes down because of the impact of the received recommendations. The obtained result is expected as the blackhole attacker drops all of received packets, however, the greyhole attacker stops forwarding some of received packets. Thus, the drop for network throughput values in blackhole attack is higher than the greyhole attack.



(a) PDR



(b) Network throughput

Figure 4.8: Network performance in the presence of malicious nodes: a) PDR; b) Network throughput

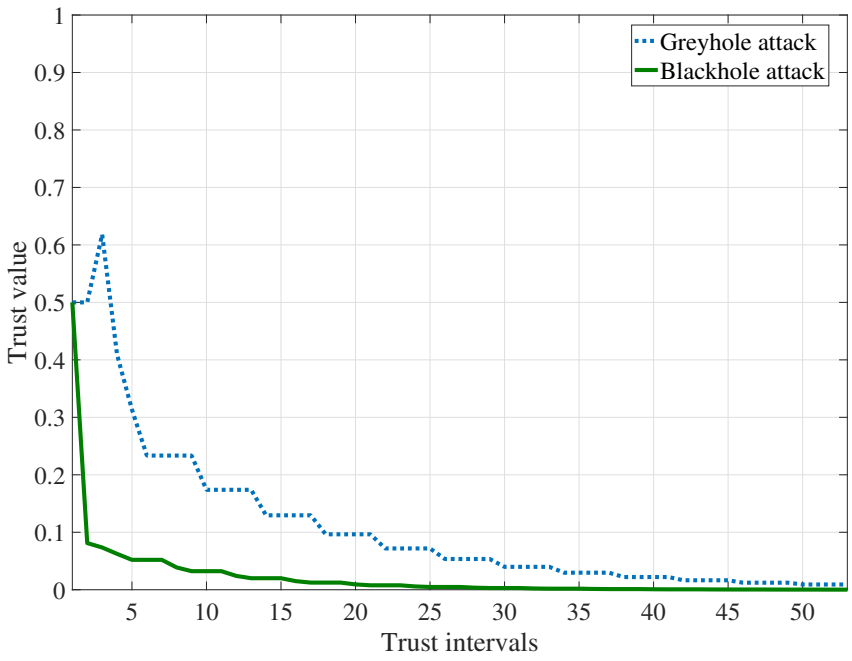


Figure 4.9: Trust values for balckhole and greyhole attackers

4.4 Theoretical Analysis

In this subsection, a theoretical analysis is presented to explain and show the performance of the proposed model and the existing model [121]. The recommendation-based trust model in [121] is used to evaluate the performance of the proposed model. Based on literature review in Chapter 3, this model is chosen because it applies very similar method to the proposed model which includes recommendation filtering and clustering. Also, weighted-sum method was implemented in the existing model. In addition, it was applied on a mobile adhoc network which has network specifications close to the vehicular network. These reasons makes it a good candidate for comparison. The model in [121] considered two trust components which are direct and indirect to filter out bogus recommendations. The total trust is computed by

$$T_{ij} = w_d \times T_{ij}^d + w_i \times T_{ij}^i \tag{4.11}$$

where T_{ij}^{d} is the direct trust, T_{ij}^{i} is the indirect trust. w_d and w_i are the weights for direct and indirect trusts, respectively, and $w_d + w_d = 1$. The calculation of direct trust (T_{ij}^{d}) is based on the beta function as follows

$$T_{ij}^{d} = \frac{\kappa_{i,j}}{\kappa_{i,j} + \tau_{i,j}} \tag{4.12}$$

where $\kappa_{i,j} = \kappa_{i,j} + \rho_{i,j}$ and $\tau_{i,j} = \tau_{i,j} + \omega_{i,j}$. The calculation of $\rho_{i,j}$ and ω would be as $\rho = \rho + 1$ when observing normal behavior (forward packet) and $\omega = \omega + 1$ when observing misbehavior (dropping packet). The indirect trust (T_{ij}^{i}) is computed as

$$T_{ij}^{i} = \sum_{e=1}^{H} \frac{\kappa'_{e,j}}{\kappa'_{e,j} + \tau'_{e,j}} \tag{4.13}$$

where H is the number of received recommendations about node j and e is the recommender node. In addition, the existing model applied three values on the received recommendations which are deviation, confidence and closeness. If the computed values applied the predefined thresholds, the received recommendation is accepted. The following case studies are proposed to compare the proposed model with the existing one theoretically.

4.4.1 Case Study 1: Evaluating Past Behavior to Reduce the Impact of Bad-mouthing Attack

The ability of node i to classify normal node j correctly in the existence of a bad-mouthing attacker is studied. In this case, the direct interaction between node i and node j exists. Also, there are recommenders about node j.

Statement 1. The proposed model is able to minimize the effect of bad-mouthing attacks.

Proof. In the *existing model*, node j behaves normally but there is a bad mouthing attack on it. Because of fake recommendations, the value of indirect trust is less than 0.5: ($T_{i,j}^{i} < 0.5$). Based on their assumptions: $w_d = 0.5$, $w_i = 0.5$ and trust threshold is equal to 0.4.

$T_{ij} \geq 0.4$ (trusted node)

$0.5 \times T^d_{i,j} + 0.5 \times T^i_{i,j} \geq 0.4$

$0.5 \times (T^d_{i,j} + T^i_{i,j}) \geq 0.4$

$T^d_{i,j} + T^i_{i,j} \geq \frac{0.4}{0.5}$

$T^d_{i,j} + T^i_{i,j} \geq 0.8$

$T^d_{i,j} \geq 0.8 - T^i_{i,j},$

Because $T^i_{i,j} < 0.5$, then $T^d_{i,j} > 0.3$ to be be able to detect the normal node correctly. Therefore, if the normal node relays more than or equal to 30% of the received packets, it is enough to be considered as trusted node. As a result, the bad mouthing attack has small impact on trust decision in the existing model while the the node behaves normally. On the other hand, in the *proposed model*, when the node j behaves normally but there is bad mouthing attack, the following conditions are considered:

1. low value of indirect trust: $T^{(t)}_{in(i,j)} < 0.5$, because all recommendations regarding *node j* are negative;
2. based on (4.8), $w_1 \rightarrow (0, 0.5]$ and $w_2 \rightarrow [0.5, 1)$;
3. from 1 and 2, $w_1 \times T^{(t)}_{in(i,j)} < 0.25$.

In the proposed model, the node is classified as normal node when $T^{(t)}_{t(i,j)} \geq 0.5$. In this case, method 2 (case 2) is applied because of the existence of direct communication and recommendations regarding node j.

$T^{(t)}_{t(i,j)} \geq 0.5$ (trusted node)

$w_1 \times T^{(t)}_{in(i,j)} + w_2 \times T^{(t)}_{c(i,j)} \geq 0.5$

$$w_2 \times T^{(t)}_{c(i,j)} \geq 0.5 - w_1 \times T^{(t)}_{in(i,j)}$$

Because $w_1 \times T^{(t)}_{in(i,j)} < 0.25$

$$w_2 \times T^{(t)}_{c(i,j)} > 0.25$$

Thus, the node takes incorrect decision regarding normal node when

$$w_2 \times T^{(t)}_{c(i,j)} \leq 0.25$$

$$w_2 \leq \frac{0.25}{T^{(t)}_{c(i,j)}} \ , \quad \text{Because } w_2 \geq 0.5$$

$$\frac{0.25}{T^{(t)}_{c(i,j)}} \geq 0.5$$

$$0.25 \geq 0.5 \times T^{(t)}_{c(i,j)}$$

The normal node is always classified as malicious node regardless of the value of indirect trust when

$$T^{(t)}_{c(i,j)} \leq 0.5$$

Therefore, $\frac{T^{(t)}_{p(i,j)} + T^{(t)}_{d(i,j)}}{2} \leq 0.5$

As a result, if the node has a good past behavior $T^{(t)}_{p(i,j)} > 0.5$ and a good direct experience $T^{(t)}_{d(i,j)} > 0.5$, the model cannot detect it incorrectly as a malicious node. As a result, there is no impact on bad mouthing attack in the proposed model.

4.4.2 Case Study 2: Evaluating Past Behavior to Reduce the Impact of Good-mouthing Attack

The ability of node i to detect malicious node j correctly with the existing of good-mouthing attack is evaluated. In this case study, the direct experience and recommendations regarding node j exist.

Statement 2. The proposed model is able to minimize the effect of a good-mouthing attacks.

Proof. Existing model: The node j behaves maliciously but there is good mouthing attack. The attacker sends good recommendations regarding malicious node j therefore, the indirect trust value of node i regarding node j is high ($T^i_{i,j} \geq 0.5$).

$$0.5 \times T^d_{i,j} + 0.5 \times T^i_{i,j} < 0.4 \text{ (malicious node)}$$

$$0.5 \times (T^d_{i,j} + T^i_{i,j}) < 0.4$$

$$T^d_{i,j} + T^i_{i,j} \geq \frac{0.4}{0.5}$$

$$T^d_{i,j} + T^i_{i,j} < 0.8$$

if $T^i_{i,j} \geq 0.8$, then the malicious node is always detected incorrectly as normal node. Otherwise, the direct trust value should achieve the following condition:

$$T^d_{i,j} < 0.8 - T^i_{i,j}$$

Therefore, as much as the indirect trust value increases, smaller value for direct trust is required to be able to detect the malicious node. Hence, the existing model is affected by good mouthing attacks. On the other hand, in the *proposed model*, when node i receives good recommendations regarding malicious node j, the following conditions are achieved:

1. good-mouthing attackers result in high indirect trust value: $T^{(t)}_{in(i,j)} \geq 0.5$.

2. based on (4.8), $w_1 \rightarrow (0, 0.5]$ and $w_2 \rightarrow [0.5, 1)$;

3. from 1 and 2, $w_1 \times T^{(t)}_{in(i,j)} \leq 0.5$.

In the proposed model, the node is classified as malicious node when $T^{(t)}_{t(i,j)} < 0.5$.

$$w_1 \times T^{(t)}_{in(i,j)} + w_2 \times T^{(t)}_{c(i,j)} < 0.5$$

$$w_2 \times T^{(t)}_{c(i,j)} < 0.5 - w_1 \times T^{(t)}_{in(i,j)}$$

Because $w_1 \times T^{(t)}_{in(i,j)} \leq 0.5$

$$w_2 \times T^{(t)}_{c(i,j)} < 0.5$$

Thus, the node takes incorrect decision by classifying malicious node as a normal node when

$$w_2 \times T^{(t)}_{c(i,j)} \geq 0.5$$

$$T^{(t)}_{c(i,j)} \geq \frac{0.5}{w_2} \ , \quad \text{Because } w_2 \rightarrow [0.5, 1)$$

$$T^{(t)}_{c(i,j)} > 0.5$$

$\frac{T^{(t)}_{p(i,j)} + T^{(t)}_{d(i,j)}}{2} > 0.5$, Then:

$$T^{(t)}_{d(i,j)} > 1 - T^{(t)}_{p(i,j)}$$

Therefore, because it is a malicious node, the direct and past trust are very small which is very rare to achieve the condition. Therefore, the impact of good-mouthing attack is very small on the proposed model unless $w_1 \times T^{(t)}_{in(i,j)} = 0.5$, where indirect trust is the highest value which equals 1 and w_1 is equal to 0.5. Finally, the value of total trust is affected by many values which are the number of recommenders, number of good-mouthing attackers and current trust value.

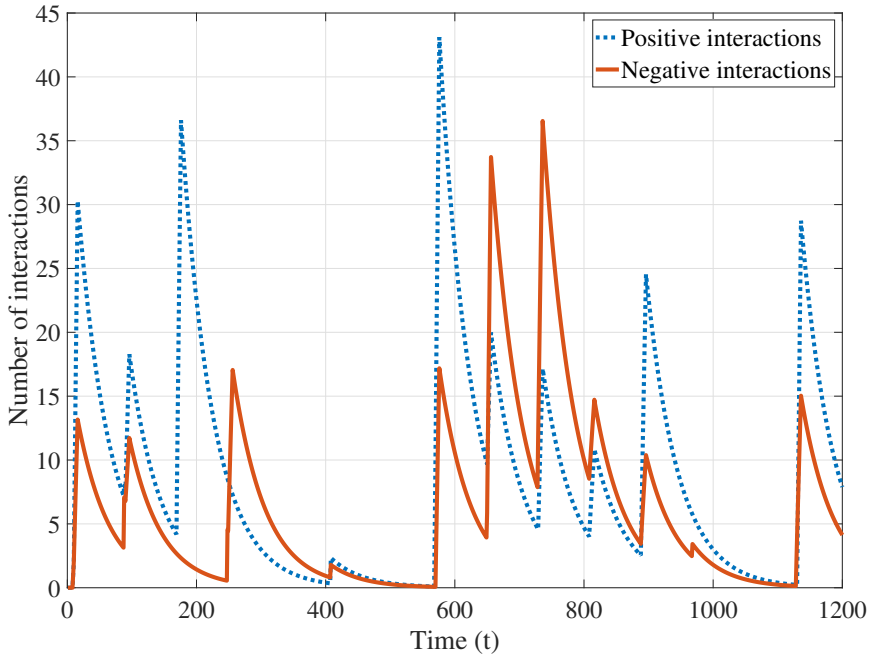


Figure 4.10: Effect of decay factor on positive and negative interaction during the simulation time

4.4.3 Case Study 3: Detecting Non-stable Malicious Behavior

Malicious nodes can escape the punishment when it stops behaving maliciously for a while. As a consequence, the ability of malicious node to return after a period of time t as a normal node is measured. In this case study, the non-stable behavior of greyhole attackers is only considered.

Statement 3. Higher detection rate for non-stable malicious nodes in the proposed model than the existing one.

Proof. The *existing model* applied decay factor (μ) on the number of interactions between node i and node j. The number of positive and negative interactions decrease with time when there is no interaction between them as shown in Figure 4.10. The number of positive and negative interactions is increased as long as there is a communication between the two nodes. Otherwise,

the number of interactions is decreased because of applying the following computation

$$\rho = \rho^{old} \times \mu, \quad \omega = \omega^{old} \times \mu$$

where ρ and ω are the number of positive and negative interactions respectively, and $0 \leq \mu \leq 1$. On the other hand, in the *proposed model*, the total trust always considers past trust when there is a previous communication with the considered node j as shown in equation 4.7. In this case, even if the malicious node leaves the area for a while to wash its past behavior. The proposed model is able to remember its past behavior.

4.4.4 Case Study 4: Rejecting Recommendations from Malicious Recommenders

To disturb trust-based model, the malicious node could send fake recommendations regarding other nodes. As a result, in this case study, the ability of node i to reject the recommendations which are sent by malicious nodes is examined.

Statement 4. The proposed trust model is able to reject the recommendations from malicious nodes.

Proof. In the *existing model*, the ability of the existing model to ignore the recommendations from malicious nodes is evaluated. The model applied various conditions on the collected recommendations, however, the node still counts recommendations from malicious nodes.

The first condition is based on the confidence value which is computed by

$$V_{ik}^{conf} = 1 - \sqrt{\frac{12\delta_{ik}\gamma_{ik}}{(\delta_{ik}+\gamma_{ik})^2(\delta_{ik}+\gamma_{ik}+1)}}$$

where δ_{ik} is the accumulative positive interactions between node i and node k, and γ_{ik} is the accumulative negative interactions between node i and node k. They are computed using

$$\delta_{ik} = \rho + 1, \quad \gamma_{ik} = \omega + 1$$

Because the multiplication and summation are reversible operations. Therefore, $V_{ik}^{conf1} = V_{ik}^{conf2}$ where

V_{ik}^{conf1} when $\delta_{ik} > \gamma_{ik}$ **and** V_{ik}^{conf2} when $\gamma_{ik} > \delta_{ik}$

Then, the confidence value is increased when the total number of interactions is increased either positive or negative interactions. Moreover, the second condition is based on the deviation value as follows:

$$\left| T_{i,j}^{d} - T_{k,j}^{d} \right| \leq 0.5$$

For example, if node j is a trusted node where ($T_{i,j}^{d} = 1$). However, node k sends bad recommendation about normal node j where ($T_{k,j}^{d} = 0.5$). In this case, the deviation condition is achieved and this recommendation is accepted. On the other hand, in the *proposed model*, during the recommendation collection phase, the node i applies the filtering process on the recommending node k. Thus, if the node k is malicious node, the confidence value $C_{(i,k)}^{(t)}$ is equal to zero and its recommendation is ignored as shown in (4.4).

4.4.5 Case Study 5: The Road Entity Travels to a New Region

As the road entity has high chance to meet new nodes in different locations while traveling, both models are evaluated when the road entity moves from its current location to a new region where there is no previous information about any road entity. Therefore, the ability of the proposed model to make a decision is studied.

Statement 5. The ability of detecting malicious nodes, when the road entity travels to a new area, in the proposed model is better than that in the existing model.

Proof. In the *existing model*, the confidence value will be zero for all recommending nodes because the confidence value for them will be as follows.

$\rho = 0, \quad \omega = 0$

$\delta_{ik} = \rho + 1 = 1, \quad \gamma_{ik} = \omega + 1 = 1 \quad \Rightarrow \; V_{ik}^{conf} = 0$

The algorithm cannot establish trustworthy cluster of recommendations. Therefore, the recommendation system fails and total trust cannot be calculated. As an assumption, if the model is able to compute the total trust based on the direct trust only, thus, $T_{i,j}^{t} = 0.5$. Therefore, node j is always considered a trusted node because the trust threshold in the existing model is equal to 0.4.

On the other hand, in the *proposed model*, when no previous interactions between node i and node j exist, the following information is considered:

1. $T_{t(i,j)}^{(t)} = T_{in(i,j)}^{(t)}$;
2. $C_{(i,k)}^{(t)} = 0.8$ because $T_{t(i,k)}^{(t)} = 0.5$ which is the initial value; as node i does not meet any of surrounding recommenders before.

Thus, the previous information is used to evaluate the ability of a normal node to detect a malicious node in a new region.

$$\frac{\sum_{k=1}^{a}[C_{(i,k)}^{(t)} \times T_{t(k,j)}^{(t)}]}{a} \geq 0.5$$

$$a \leq \frac{\sum_{k=1}^{a}[C_{(i,k)}^{(t)} \times T_{t(k,j)}^{(t)}]}{0.5}$$

The node is trusted only if the value of a is located in the valid range.

4.5 Performance Evaluation

This subsection evaluates the performance of the proposed model with weighted-sum method in comparison with the existing one [121]. The performance of the trust model is studied with respect to three main metrics which are FNR, recommendation usage rate and prediction rate. In addition, the network performance is measured by calculating the improvement in PDR and network throughput. Also, various malicious patterns are examined.

4.5.1 Evaluation of Trust Model Performance

False Negative Rate

It is the rate of undetected malicious nodes. As long as the model has a low FNR, the impact of malicious nodes is minimal. High FNR means that the malicious node stays in the network for a long time without being detected. The result that is shown in Figure 4.11 represents the FNR for various percentages of malicious nodes. The following remarks can be made:

- in the existing model, as the percentage of malicious nodes increases, FNR rises significantly.
- In comparison with the existing model, the FNR is increased slightly in the proposed model. Thus, the malicious node is detected faster in the proposed model than the existing one.
- When the percentage of malicious nodes is high, the FNR in the proposed model is still

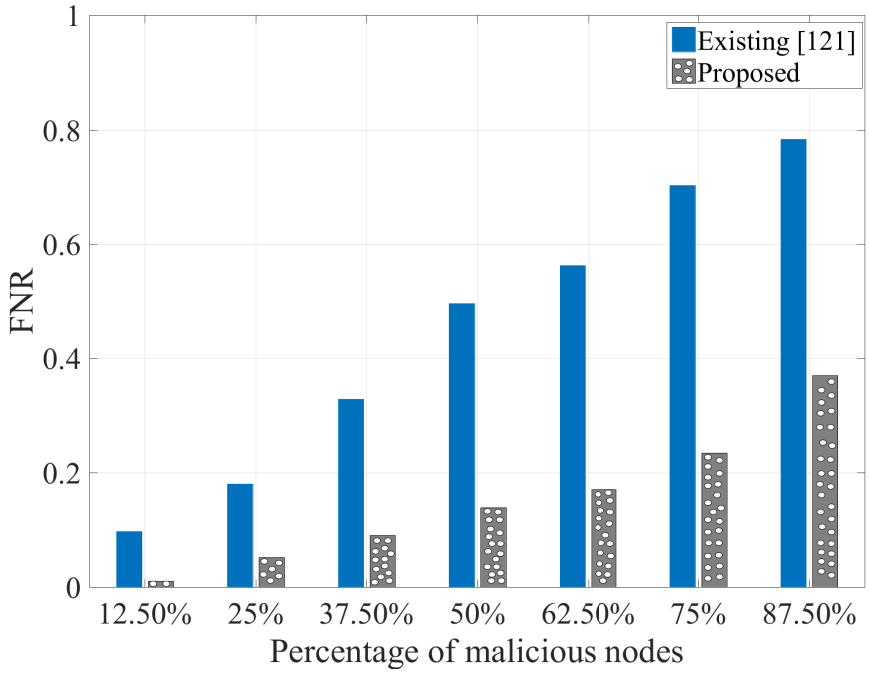


Figure 4.11: False negative rate with various percentage of malicious nodes

lower than 0.4.

Recommendation Usage Rate

The recommendation usage rate is critical in the vehicular network because of the high chance of meeting a new entity. When the vehicle does not have enough information about the new entity, it leads to wrong decisions. Thus, the received recommendations could minimize the incorrect decisions.

As a result of the recommendation attacks, the node has to check the trustworthiness of the recommendation source. The node only accepts the recommendations from trusted neighbors.

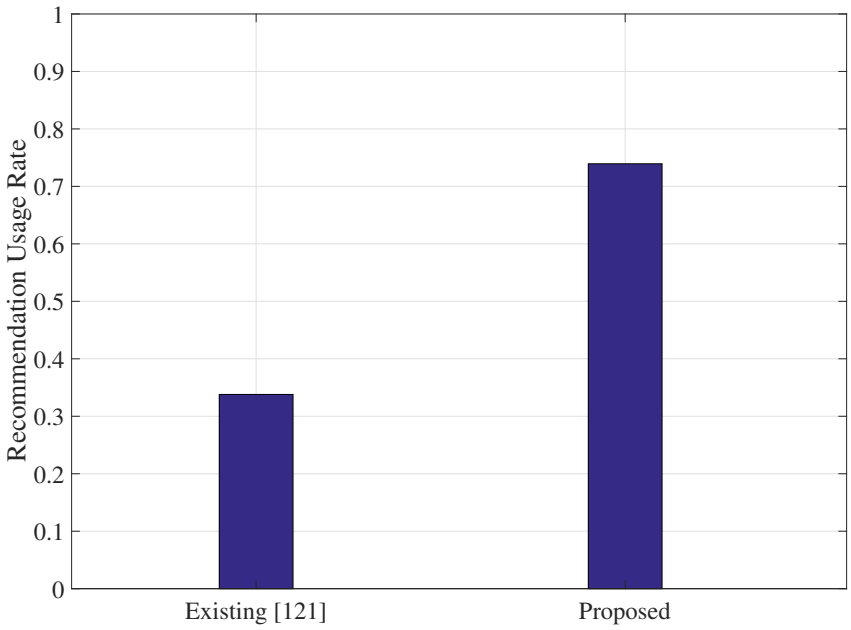


Figure 4.12: Recommendation usage rate in the proposed and exiting models

Recommendation usage rate is calculated using

$$Recommendation\_Rate = \frac{Count\_Recommendations}{Total\_Calculations} \tag{4.14}$$

where $Count\_Recommendations$ is the times of using recommendations in trust calculations and $Total\_Calculations$ is the total number of trust calculations. On the other hand, the existing model [121] applied various conditions for taking the recommendations which lead to ignore the most of recommendations or accept fake recommendations. Therefore, the recommendation usage rate in the existing model is less than the proposed one as shown in Figure 4.12, which means that the existing model does not take advantage of using recommendations as much as the proposed model.

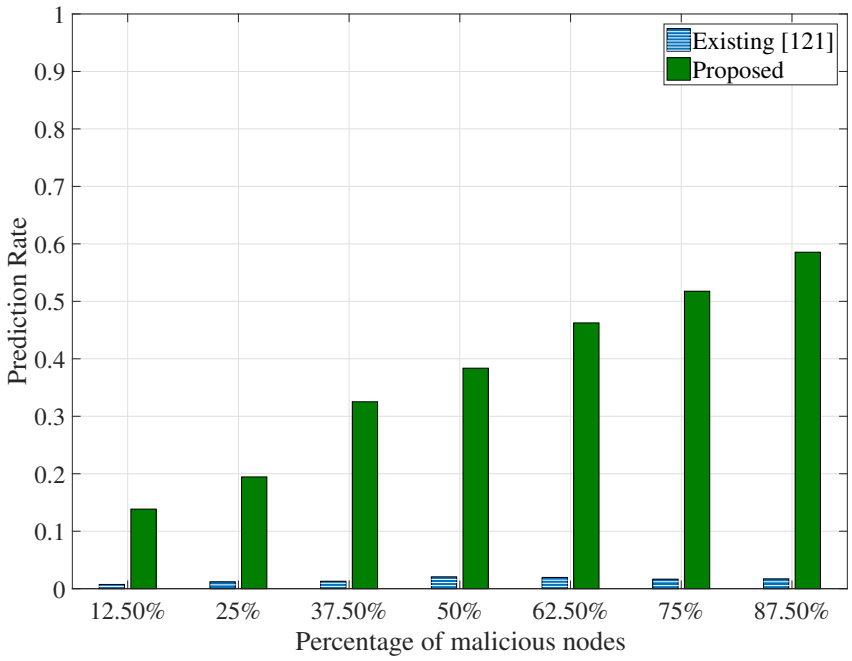


Figure 4.13: Prediction rate with various percentage of malicious nodes

Prediction Rate

Prediction rate is the rate of avoiding the first communication with malicious nodes. When the node moves to a new location, it needs for the recommendations from the neighboring nodes to have awareness regarding the neighboring malicious nodes and avoid the communication with them. As a result of the high recommendation usage rate in the proposed model, the nodes are able to predict and detect malicious nodes before communicating with them as shown in Figure 4.13. The main reason for the huge difference for prediction rate in both models is because of the strict condition and limitations for accepting recommendation in the existing model. For instance, case study 5 in previous subsection presented the limitation in collecting recommendations when the vehicle travels to a new region. Also, case study 4 showed that the entity could accept malicious recommendations which could affect on final decision. Thus, the proposed model improves the network performance by addressing the gaps in the existing model.

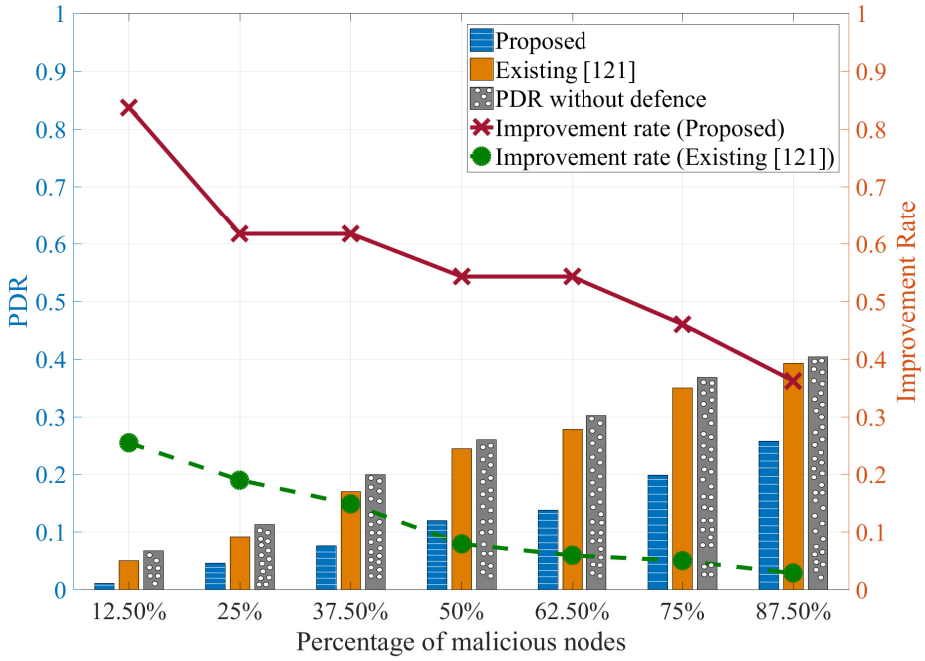


Figure 4.14: Improvement rate in PDR with various percentage of malicious nodes

4.5.2 Evaluation of Network Performance

The performance of the entire network is represented by PDR and network throughput in the presence of malicious nodes. PDR is evaluated to see the impact of such attacks with and without trust models. Also, the improvement rate for both models are measured in comparison with the network without defense model. As shown in Figure 4.14, the PDR value in the proposed model is low in comparison with the network without defense. When the percentage of malicious nodes is less than 50%, the PDR is very low which is less than 10% of the received packets. This clarifies the high improvement rate of the proposed model in the network performance. On the other hand, PDR for the existing model is high and close to the values when the network without defense. Thus, it achieves lower improvement rate. In addition, PDR in the proposed model is improved to reach 84% when the percentage of malicious nodes is less than or equal to 12.5%. On the contrary, the exiting model only achieves 25%.

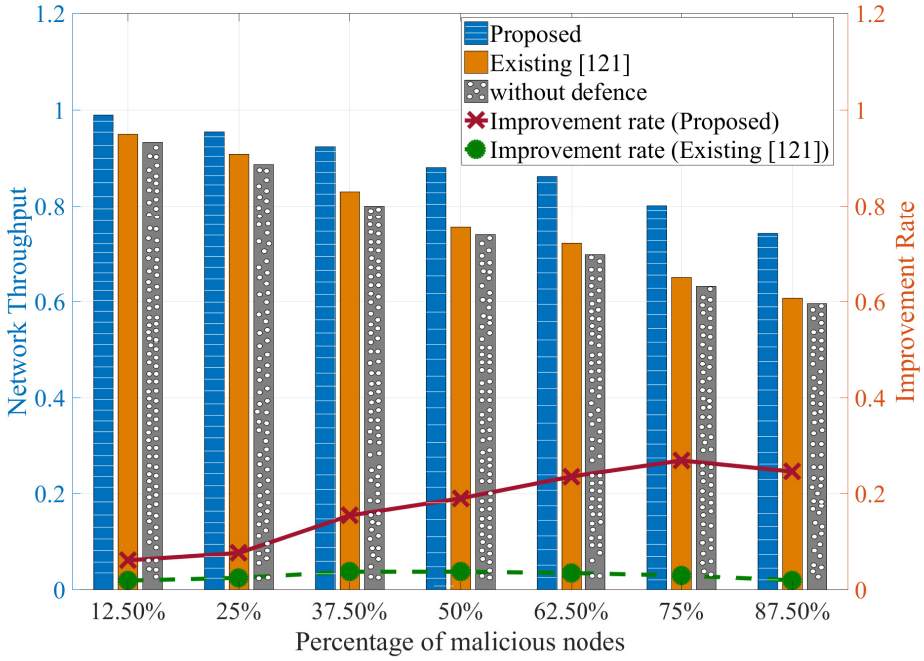


Figure 4.15: Improvement rate in network throughput with various percentage of malicious nodes

Moreover, the network throughput is measured with and without trust models. As shown in Figure 4.15, the network throughput in the proposed model is the highest which leads to an improvement in the network performance. On the other hand, the network throughput for the existing model is very close to the network without defense. In addition, the improvement rate in network throughput in the proposed model is increased when the percentage of malicious nodes is increased.

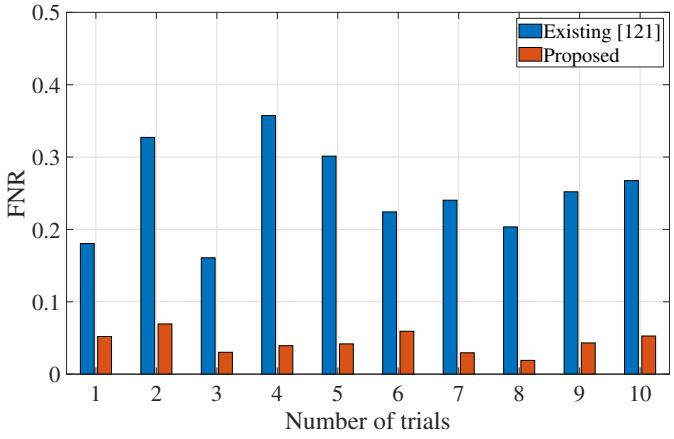
4.5.3 Study the Randomness of Malicious Nodes

Here, the impact of random choice of malicious nodes is studied. Each trial different 6 malicious nodes is defined. In Figure 4.16 (a), the change of choosing malicious nodes in the proposed model has a small difference of FNR values. However, the FNR values has bigger variation in the existing model. In addition, in Figure 4.16 (b), the PDR values for most of trials in the proposed model are less than 0.05. On the other hand, the PDR values in some trials reach to 0.18 in the existing model.

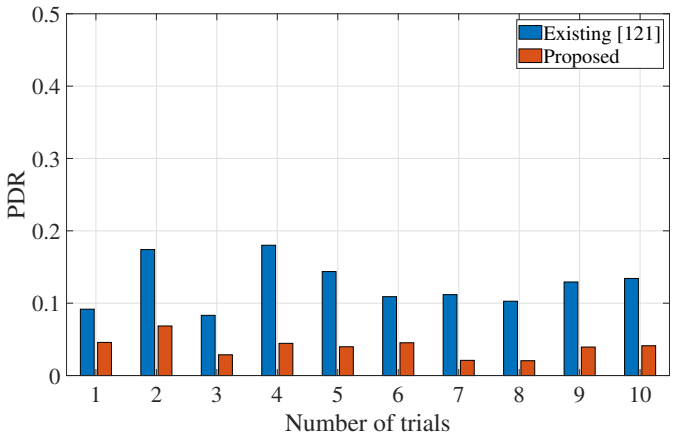
4.5.4 Performance Comparison for Stable Malicious Behavior

The model performance is studied in the case of stable malicious nodes. The malicious node behaves maliciously in a continuous manner during the whole simulation time. Here, the trust computation for the malicious node is done in each interval even if after it is classified as a malicious node to study its malicious behavior. From Figure 4.17, the following remarks are summarized:

- In the existing model, the trust values are volatile even though the stable malicious behavior. The reason behind that is the effect of the decay factor which allows for decreasing the positive and negative interactions when there is no communication. Therefore, the trust value goes up again during the period of non-communication. Thus, the malicious node can gain high trust values where the trust threshold in the existing mode is equal to 0.4. In addition, the malicious node is considered as a normal node for first ten intervals.



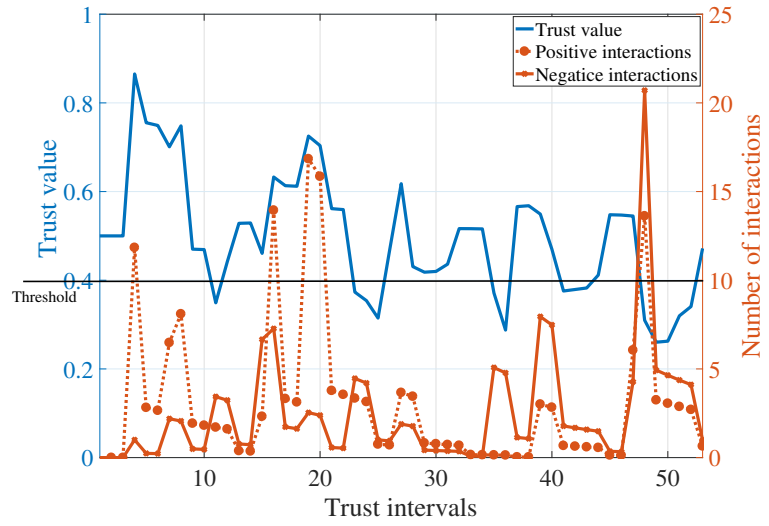
(a) FNR



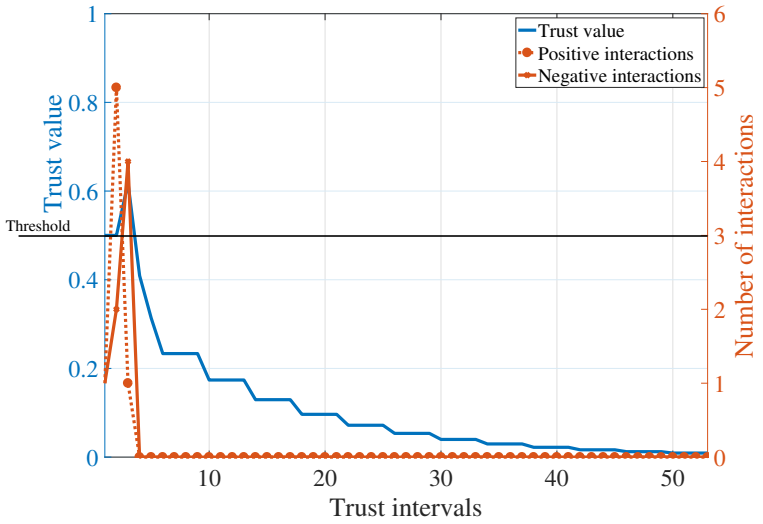
(b) PDR

Figure 4.16: Study the impact of the randomness in choosing the malicious nodes: a) FNR; b) PDR

- On the other hand, in the proposed model, the trust value in the proposed model is more consistent than the existing model. At the beginning, the value increases because of the behavior of the greyhole attacker. Then, it gradually decreases over the time because when no communication is established for a period, the number of interactions is zero. Thus, the trust value is computed based on the past trust and the recommendations values. In



(a) Existing model [121]



(b) Proposed model

Figure 4.17: Performance comparison for stable malicious behavior: a) Existing model [121]; b) Proposed model

addition, the malicious node is detected after a short time which is around the 4^{th} interval.

4.5.5 Performance Comparison for Non-stable Malicious Behavior

The model performance in the existence of non-stable malicious nodes is evaluated in comparison with the existing model. From the result in Figure 4.18, the following points are concluded:

- in Figure 4.18 (a), the malicious node behaves normally between 1-15 time intervals. Therefore, the trust values are increased during these intervals in both models. After the 15^{th} interval, the trust value drops in the proposed model more than the existing model. The reason for non-steady trust values before the 15^{th} interval is the effect of the recommendations. If the node receives recommendations regarding the malicious node, the trust value goes down. Otherwise, the trust value only depends on the direct experience which means high trust value.

- in Figure 4.18 (b), the malicious node behaves normally between 15-35 time intervals. However, the normal behavior of the malicious node does not affect the trust value in the proposed model. The reason for that is the impact of past behavior on the trust value. On the other hand, in the existing model, the trust value is gradually increased after the 15^{th} interval because of many reasons which are low recommendation usage rate and the impact of the decay factor.

- in Figure 4.18 (c), the malicious node behaves normally between 35-53 time intervals. The trust value in the proposed model is not affected. On the other hand, the trust value in the existing model is gradually increased after the 35^{th} interval, but it is in a lower value than the previous case.

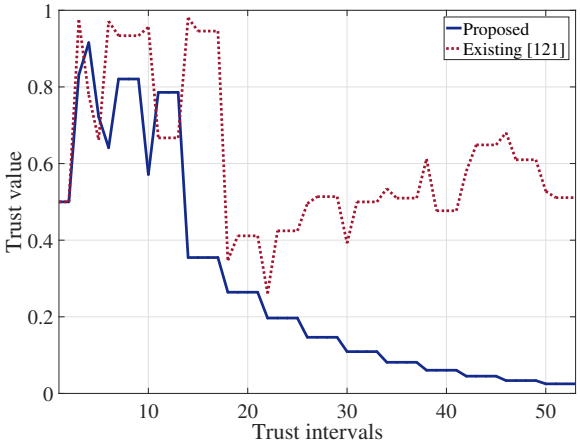
- in conclusion, the proposed trust model is less affected by non-stable malicious behavior than the existing model.

4.6 Summary

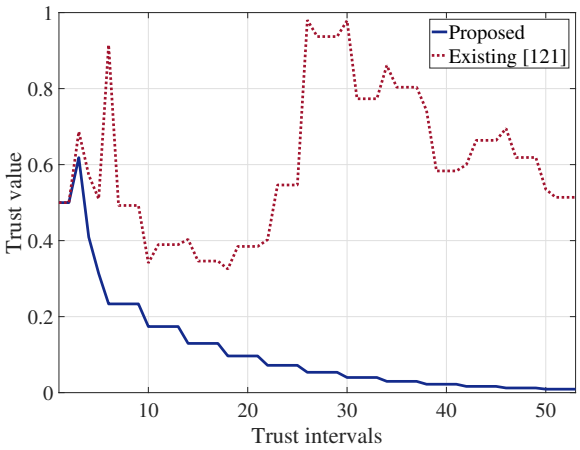
In this chapter, a recommendation-based trust model for the V2X network was proposed. Various trust parameters are maintained, which are direct, past and indirect trust. The proposed model suggested an adaptive weight in the recommendation filtering process. The weights are changed based on the number of positive and negative recommendations. Thus, the effect of the recommendation attacks is reduced. Also, various malicious attacks were examined, which are blackhole attack, greyhole attack, bad-mouthing attack and good-mouthing attack. Also, various malicious patterns were applied, such as stable and non-stable malicious behavior. Moreover, many experiments were conducted to study the performance of the proposed model. Also, the effect of various percentage of malicious nodes on multiple metrics was studied. A theoretical analysis for both models was presented to show the outperformance of the proposed model by studying five case studies with different scenarios. In addition, the simulation results showed that the proposed model surpasses the existing model. The main conclusions are:

- The proposed model benefited from the neighboring recommendations more than the existing model. In the existing model, most of the recommendations are discarded because of confidence and deviation thresholds. However, the recommendation usage rate for the proposed model is around 75%.
- The proposed model improved the network performance by achieving low PDR in comparison with the network without defense system. The improvement rate reaches to 36% for the maximum percentage of malicious nodes.
- The network throughput was improved by the proposed model by an average percentage greater than or equal to 20% when the percentage of malicious nodes is greater than or equal to 50%.
- Stable malicious behavior was detected easily in the proposed model because of the impact of past trust. However, because of the variation in positive and negative interactions in the existing model, trust values could rise again after a while.

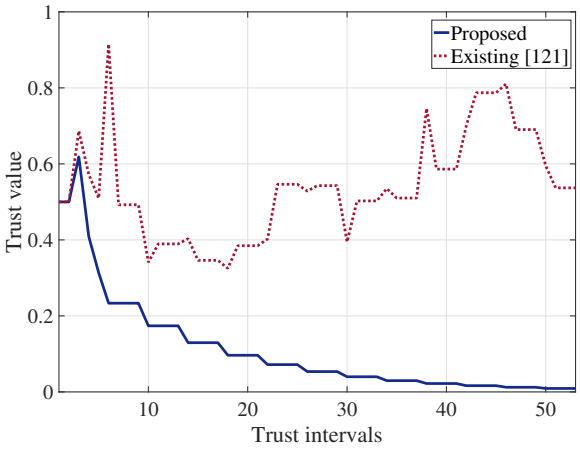
- The detection of stable malicious behavior in the proposed model is quicker than the existing model. Thus, the network performance in the proposed model is better.
- In non-stable malicious behavior, when the malicious node starts behaving maliciously at the beginning of the simulation time, both models were affected and gained high trust values because there is no past trust for that node. However, if the malicious node starts with malicious behaviors then after a while behaves normally, the trust values in the proposed model is not affected.



(a) Normal behavior between time interval 1 and 15



(b) Normal behavior between time interval 15 and 35



(c) Normal behavior between time interval 35 and 53

Figure 4.18: Performance comparison for non-stable malicious behavior

Chapter 5

Global Roaming Trust-based Model for V2X Communication

As the road entities move and travel to various regions, the chance to meet new entities is very high. When the road entity meets a new entity, based on the proposed trust-based model in Chapter 4, the trust is measured based on the surrounding entities' opinion. However, the trust value is not accurate when the surrounding entities do not have any information regarding that new entity. To improve the decision accuracy, this chapter achieves Objective 3 in Chapter 1 by developing the proposed model in Chapter 4 to have global roaming ability which solves Gap 1.4 in Chapter 2. In addition, Gap 1.3 is addressed where the enhanced model can protect the network against RSU attacks.

This chapter proposes the global roaming trust-based model that gives the road entities global knowledge regarding malicious nodes in the network. As much the entity is connected with the core network, it receives the updated global blacklist. Otherwise, it applies the local blacklist, which is based on the trust-based model in Chapter 4. The central server has the responsibility to

make the global decision and reduce the impact of various RSU attacks. Also, various experiments are conducted with different percentage of malicious road entities and RSUs to measure the performance of the proposed model.

5.1 Proposed System Model

This subsection presents details regarding the considered network. Also, various attacks on road entities and RSUs are explained.

5.1.1 The Considered Network

The considered network consists of N road entities, which move at various speeds, and M fixed RSUs. Each road entity sends three types of messages: *Beacon message* which is sent periodically to inform the surrounding nodes about its current speed, location and direction; *transaction message* which contains confidential information and it is sent to the core network; and *warning message* that is sent by road entities to the surrounding RSUs when a malicious behavior is detected. Moreover, the considered network has two types of road entities which are normal and malicious entities. The normal entity keeps monitoring the surrounding entities, sends its packets to the core network and relays any received packet to the nearest RSU. In addition, the road entity is able to evaluate the trustworthiness of the surrounding entities. Based on its decision, it can generate two types of warning messages which are *malicious alarm* and *uncertain alarm*. On the other hand, the malicious entity launches various attacks to disturb the network performance such as:

- Selective forwarding attack: occurs when the malicious entity drops some of the received packets randomly to escape punishment.
- Recommendation attack: occurs when the malicious entity sends bogus recommendations regarding other entities such as good-mouthing attack and bad-mouthing attack which described in details in Chapter 4.

Moreover, based on the literature review in Chapter 2, much research considered RSUs as trusted nodes in the network. However, they are vulnerable to various cyber-attacks. Thus, ignoring their malicious behavior could destroy the network and affect the trust decision. As a result, two types of RSUs are considered as follows:

- *Normal RSU:* keeps receiving the warning messages and makes a decision based on the volume of warning messages. Then, it sends its decision to the central server.
- *Malicious RSU:* initiates malicious behavior to disturb the network such as bad-mouthing attack where the RSU sends malicious warning to the central server regarding normal nodes; and good-mouthing attack where the RSU drops the malicious warning regarding other malicious nodes.

5.2 The Proposed Model

The global roaming trust-based model maintains two levels of trust as shown in Figure 5.1 which are *road entities level* and *RSU level*. In road entity level, each entity evaluates the trustworthiness of surrounding entities, and sends warning messages to the surrounding RSUs when a malicious behavior is detected. When the RSUs received high volume of warning messages from the surrounding entities (RSU level), they generate an alarm and send it to the central server. The details of this model are presented as follows.

5.2.1 Road Entity Level

During time interval t, each road entity measures the trustworthiness of all surrounding entities. In details, node i continuously monitors its one-hop neighbors j. Then, node i is able to compute current trust using the collected information. In addition, node i sends recommendation requests to the surrounding nodes k regarding node j. The proposed model manages two trust components as follows.

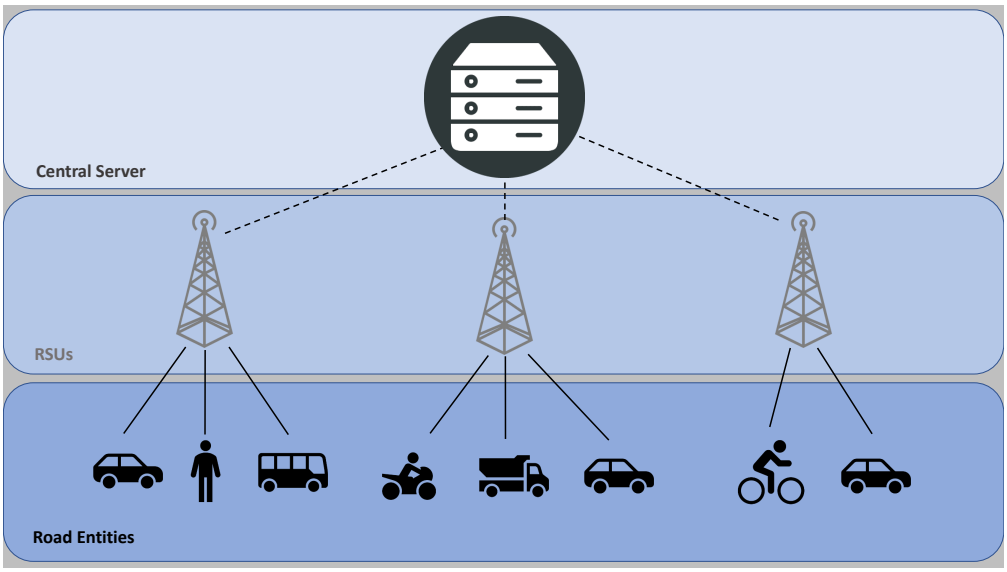


Figure 5.1: Trust levels in the proposed model

- **Current Trust -** $T^{(t)}_{c(i,j)}$: it is computed by node i to evaluate the communication experience with node j during time interval t. It is calculated using (4.1) in Chapter 4.

- **Indirect Trust -** $T^{(t)}_{in(i,j)}$: it is a measure for the behavior of neighboring nodes j using surrounding nodes' opinions. Node i collects recommendations from the surrounding nodes regarding node j. Before computing indirect trust, node i applies the following steps:

  – *Confidence value computation-* $C^{(t)}_{(i,k)}$: node i measures the confidence value for each recommender node k. $C^{(t)}_{(i,k)}$ is computed by

$$C^{(t)}_{(i,k)} = \begin{cases} 1, & \text{if } T^{(t)}_{l(i,k)} \geq Th_{max}. \\ C_w, & \text{if } Th_{min} \leq T^{(t)}_{l(i,k)} < Th_{max}. \\ 0, & \text{if } T^{(t)}_{l(i,k)} < Th_{min}. \end{cases} \tag{5.1}$$

  where C_w is the confidence weight for uncertain recommendations.

  – *Recommendations clustering*: node i classifies the received recommendations into two

groups which are positive and negative recommendations using Th_{min}. Then, node i collects recommendations by applying Algorithm 4.1 in Chapter 4.

After that, each node i calculates indirect trust for node j using (4.5) in Chapter 4.

- **Local Trust -** $T_{l(i,j)}^{(t)}$: each node i is able to compute local trust for node j and make a decision. Generally, local trust is computed in the same way that total trust is computed in Chapter 4.

- **Local decision**: node i has a local blacklist which has a list of malicious nodes based on the local decision. Thus, node i stops the communication with any node j in its blacklist. The decision is made using

$$D_{Local} = \begin{cases} Trusted, & \text{if } T_{l(i,j)}^{(t)} \geq Th_{max}. \\ Uncertain, & \text{if } Th_{min} \leq T_{l(i,j)}^{(t)} < Th_{max}. \\ Malicious, & \text{if } T_{l(i,j)}^{(t)} < Th_{min}. \end{cases} \tag{5.2}$$

where Th_{min} and Th_{max} are minimum and maximum trust thresholds, respectively. After that, the node updates its local blacklist and sends malicious and uncertain warning messages to the surrounding RSUs.

5.2.2 RSU Level

During time interval t, the nodes send malicious or uncertain warning messages based on their local decision to the surrounding RSUs. During time interval t', where $t' > t$, RSUs start trust calculation phase. First, each RSU measures the rate of malicious and uncertain alarms regarding node j using

$$M_{(j)} = \frac{mc_j}{t'}, \qquad U_{(j)} = \frac{uc_j}{t'} \tag{5.3}$$

where mc_j and uc_j are the number of malicious and uncertain warnings respectively. Second, each RSU is able to make the decision regarding node j using

$$Decision_{(RSU,j)} = Rate_{M(j)} - Rate_{U(j)} \tag{5.4}$$

```
1: for each RSU do
2:   for each RSU.warningList do
3:     w ← RSU.warningList(index)
4:     if w.NotDuplicated() then
5:       if w.isMalicious then
6:         mc_j ← mc_j + 1
7:       else
8:         uc_j ← uc_j + 1
9:       end if
10:    end if
11:  end for
12:  for each Node j do
13:    Decision_(RSU,j) ← (M_(j) − U_(j)) / (M_(j) + U_(j))
14:    if Decision_(RSU,j) > 0 then
15:      Send alarm to the central server
16:    end if
17:  end for
18: end for
```

Algorithm 5.1: Algorithm for decision computation on RSU level

where $Rate_{M(j)}$ and $Rate_{U(j)}$ are the rates of malicious alarms and uncertain alarms respectively. $Rate_{M(j)}$ is calculated by

$$Rate_{M(j)} = \frac{M_{(j)}}{TM_{(j)}} \tag{5.5}$$

where $TM_{(j)} = M_{(j)} + U_{(j)}$ and $Rate_{U(j)} = 1 - Rate_{M(j)}$.

Finally, the RSU applies Algorithm 5.1 to make a decision regarding node j. Therefore, if node j is classified as malicious node, the RSU sends malicious alarm to the central server. The time complexity for the algorithm on the node level is equal to the proposed computation in Chapter 4. In the RSU level, the complexity is equal to $O(list_{size})$ for counting the uncertain and malicious warnings. $list_{size}$ is the size of warning list that is received by the RSU. Then, each RSU computes the decision regarding all neighboring nodes. The time complexity for decision computation is equal to $O(N_{RSU})$ where N_{RSU} is the number of nodes that are connected to a specific RSU.

5.2.3 Global Trust Decision

At this stage, the central server makes the global decision regarding node j based on the alarms which are received from RSUs. The decision is made by

$$D_{Global} = \begin{cases} Malicious, & A_m > Th_G. \\ Normal, & A_m \leq Th_G. \end{cases} \tag{5.6}$$

where A_m is the number of malicious warnings that are received regarding node j and Th_G is the global trust threshold. Node j is added to the global blacklist when it is classified as malicious node. Then, the central server broadcasts the updated global blacklist to RSUs. Then, RSUs rebroadcast it again to all roads entities that are covered by the network. The road entities update their local blacklist based on the received global blacklist.

5.3 Simulation Analysis

This subsection describes the simulation set-up for evaluating the performance of the proposed model. The effect of changing parameters on the false alarm rate is also analyzed. In addition, the optimal values for various thresholds are selected.

5.3.1 Network Specifications

A V2X network is considered with 24 road entities and 9 RSUs with parameters as shown in Table 5.1. The road entities move over an area of 800×800 m^2 with various speed ranges as shown in Table 3.4. The considered area is composed of two intersections using three two-lanes roads. The road entity sends the transaction message to the core network directly or using a multi-hop routing protocol. To measure the performance of the proposed trust model, various types of malicious nodes are studied: six selective forwarding attackers, three good-mouthing attackers and three bad-mouthing attackers.

Table 5.1: Simulation parameters for studying the performance of global roaming trust-based model

Parameter	Value
Simulation time	100 iteration
Number of nodes	24 nodes
Th_{max}	0.7
Th_{min}	0.4
Th_G	3
RC	0.3
C_w	0.9
$T^{(0)}_{l(i,j)}$	0.5

Table 5.2: FNR and FPR for various values of minimum threshold (Th_{min})

Minimum threshold (Th_{min})	FNR	FPR
0.4	**0.0458**	**0.0886**
0.5	0.0641	0.3159
0.6	0.2816	0.9716
0.7	0.2786	0.9716
0.8	0.2786	0.9716
0.9	0.2786	0.9716

5.3.2 Experiment Results

The impact of changing parameters on false alarm rate is studied. False alarm rate includes FNR and FPR. FPR measures the rate of classifying normal nodes as malicious. The simulation is started using the initial parameters $Th_{max} = 0.9, RC = 0.3, C_w = 0.9$. Then, their values are updated with the optimal ones.

Study the impact of trust thresholds on false alarm rate

The simulation experiments are run with initial parameters. The impact of various values of Th_{min} on false alarm rate is studied. Also, the experiment helps to define the optimal value for Th_{min}. The corresponding results are shown in Table 5.2. The following remarks can be made:

Table 5.3: FNR and FPR for various values of maximum threshold (Th_{max})

Maximum threshold (Th_{max})	FNR	FPR
0.4	0.0535	0.0638
0.5	0.0535	0.0638
0.6	0.0458	0.0745
0.7	**0.0458**	**0.0745**
0.8	0.0458	0.0814
0.9	0.0458	0.886

- FNR and FPR values increase when the value of Th_{min} increases; however, the increase of FPR is significant.
- the impact of Th_{min} is high on FPR because as long as Th_{min} goes up that means the malicious range is expanded. As a result, many normal nodes are classified as malicious nodes;
- when $Th_{min} = 0.4$, it achieves lowest values of FNR and FPR.

Moreover, the impact of various values of Th_{max} on false alarm rate is studied. The experiment is run with initial parameters and $Th_{min} = 0.4$. As shown in Table 5.3, the FNR slightly decreases when the value of Th_{max} increases. As long as the value of Th_{max} increases, the range for normal behavior decreases. Thus, the chance of classifying the malicious node as a normal one is low. On the other hand, the FPR slightly goes up as long as Th_{max} increases because the uncertain range increases when the value of Th_{max} increases. Thus, some normal nodes could be considered as uncertain nodes which could result in a global malicious alarm. The initial value of Th_{max} is updated with 0.7 which is the optimal value.

Study the impact of recommendation factor (RC) on false alarm rate

The simulation experiments are run with updated/initial parameters. Here, the effect of various values of RC on the false alarm rate is studied. By inspecting Table 5.4, the following remarks can be made:

Table 5.4: FNR and FPR for various values of recommendation factor (RC)

Recommendation factor (RC)	FNR	FPR
0.1	0.0458	0.0745
0.2	0.0458	0.0745
0.3	**0.0458**	**0.0745**
0.4	0.0458	0.0745
0.5	0.0458	0.0851
0.6	0.0466	0.1085
0.7	0.0474	0.1340
0.8	0.0524	0.2220
0.9	0.0566	0.2724

- FPR goes up when the value of RC increases to reach approximately 0.27, however, the FNR is stable while RC increases;
- the RC has an impact on FPR only because RC is a part of the calculation of indirect trust weight w_1. Therefore, giving high weight to indirect trust results high FPR. As a result, the model starts making false decisions regarding the normal nodes.
- 0.3 is chosen as an optimal value for RC which is the same as the initial value.

Study the impact of confidence weight (C_w) on false alarm rate

Various values of C_w are examined to choose the value that achieves minimum false alarm rate, as shown in Table 5.5. Key findings are:

- FPR goes down when the C_w increases because the lower weight for the recommendations, that are sent by uncertain nodes, is given. However, the FNR decreases slightly when the C_w increases;
- the majority of normal nodes are classified as uncertain, thus, giving recommendations low weight results in high FPR.
- the initial value of C_w is the optimal one which is equal to 0.9.

Table 5.5: FNR and FPR for various values of confidence weight (C_w)

Confidence weight (C_w)	FNR	FPR
0.1	0.1263	0.6041
0.2	0.1106	0.5703
0.3	0.1011	0.5359
0.4	0.1010	0.5121
0.5	0.0770	0.4153
0.6	0.0718	0.3080
0.7	0.0653	0.2497
0.8	0.0653	0.0745
0.9	**0.0553**	**0.0638**

Study the impact of global decision threshold (Th_G) on false alarm rate

Moreover, the impact of various values of global threshold on the false alarm rate is studied. The global threshold is between 1 and 9, which represents the number of RSUs in the network. As shown in Table 5.6, the FNR increases when the threshold increases because the node is classified as a malicious node when the number of malicious warning is greater than the global threshold. Therefore, the central server should receive nine malicious warnings in case of threshold is equal to 9. On the other hand, FPR is stable until the threshold becomes greater than or equal to 7. The FPR is equal to zero when high value of threshold is considered because the honesty

Table 5.6: FNR and FPR for various values of global decision threshold (Th_G)

Global decision threshold (Th_G)	FNR	FPR
1	0.0212	0.0638
2	0.0216	0.0638
3	**0.0219**	**0.0638**
4	0.0258	0.0638
5	0.0535	0.0638
6	0.0535	0.0638
7	0.0860	0
8	0.0860	0
9	0.0860	0

of the received malicious warning is ensured. As a result, the effect of bad-mouthing attack is controlled. The choosing of optimal value should consider the balance between FNR and FPR values. Thus, $Th_G = 3$ is the optimal value which achieves low FNR and acceptable value of FPR.

5.3.3 Study the Impact of RSU Attacks

The experiments are conducted to study the impact of malicious behavior of RSUs on various metrics which are FNR, FPR and PDR. In this study, the bad-mouthing attackers send fake recommendations regarding four normal road entities.

Bad-mouthing attacks

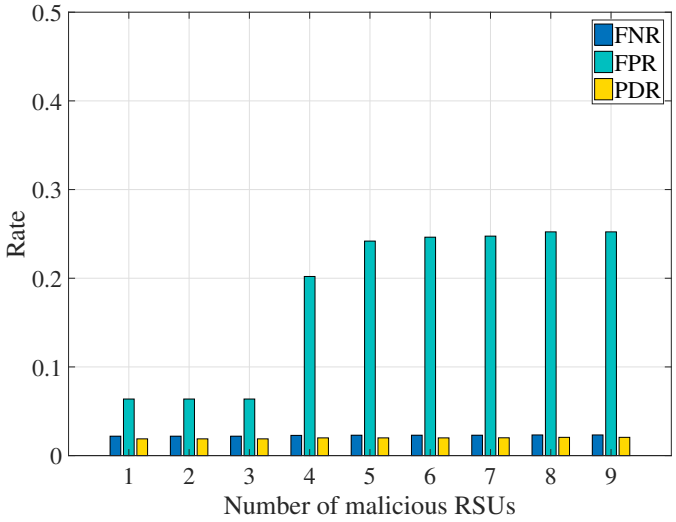
The impact of various number of malicious RSUs, which launch bad-mouthing attack, on the proposed model is studied. As shown in Figure 5.2 (a), the FPR values goes up when the number of malicious RSUs increases. The increasing starts when the number of malicious RSUs is greater than or equal to 4. On the other hand, the FNR and PDR are not affected and remains stable for various number of malicious RSUs.

Good-mouthing attacks

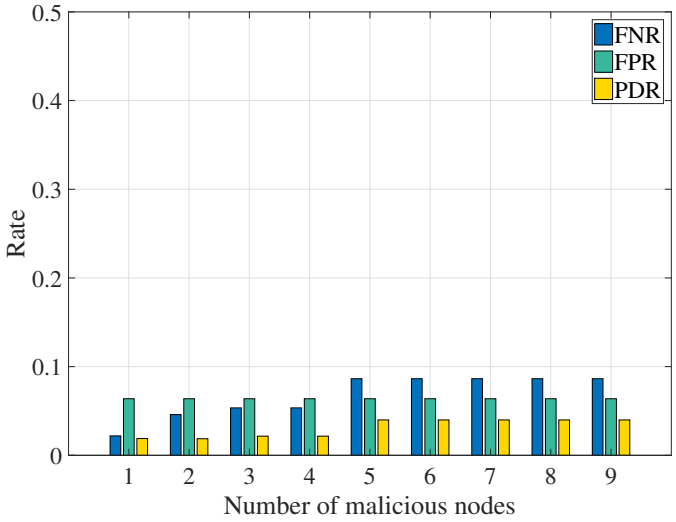
The impact of various number of malicious RSUs, which launch good-mouthing attack, on the proposed model is examined. As shown in Figure 5.2 (b), the FNR value increases when the number of malicious RSUs rises. As a result of incorrect decisions regarding malicious node, the PDR value increases. On the other hand, the FPR is not affected and remains stable for various number of malicious RSUs.

5.3.4 Study the Improvement in Trust Model with a Global Decision System

An experiment is conducted to study the improvement rate in the global decision system. The local blacklist is evaluated on each node at the end of simulation and the rate of undetected



(a) Bad-mouthing attack



(b) Good-mouthing attack

Figure 5.2: Effect of RSUs attacks on FNR, FPR and PDR: a) Bad-mouthing attack; b) Good-mouthing attack

malicious nodes is measured. Also, the ability of nodes to detect malicious nodes, when a global decision system is applied, is evaluated. As shown in Figure 5.3, the rate in distributed level varies in each node because of the different local decision, which is based on the road entity as in (5.2). In addition, the rate is very high and reaches to 1 in some nodes because the normal node does not meet the malicious node during the simulation time. However, all nodes have the same rate in the global decision level because of the global knowledge of malicious nodes even if they do not meet.

In addition, a comparison between global decision and distributed decision in equation 5.2 is studied. As shown in Figure 5.4, low FNR value is achieved by global decision where the node can avoid the communication with malicious node even if they meet for the first time. Thus, the improvement rate reaches approximately 74%. As a result of lower FNR, the PDR value is also

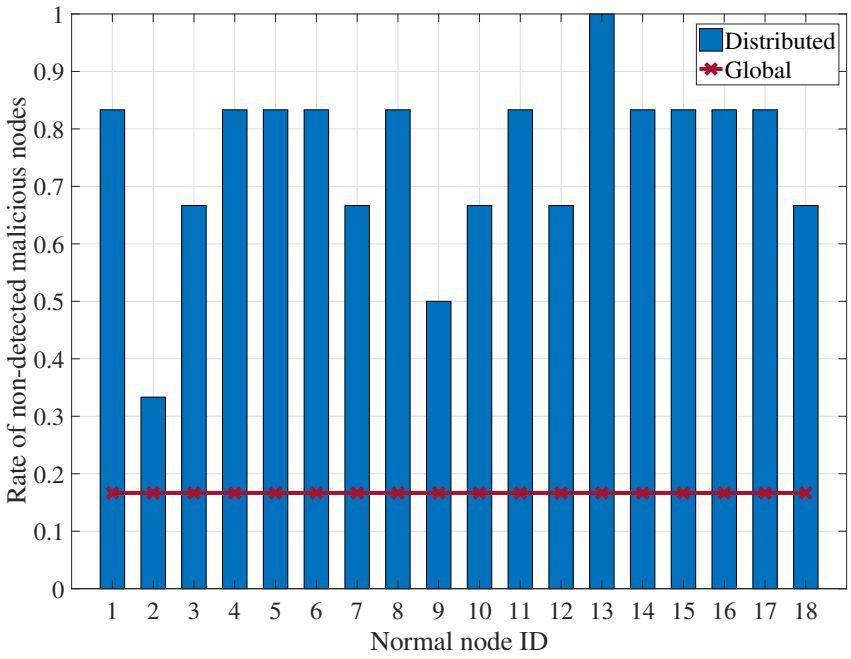


Figure 5.3: Rate of non-detected malicious nodes per node for global and distributed decisions

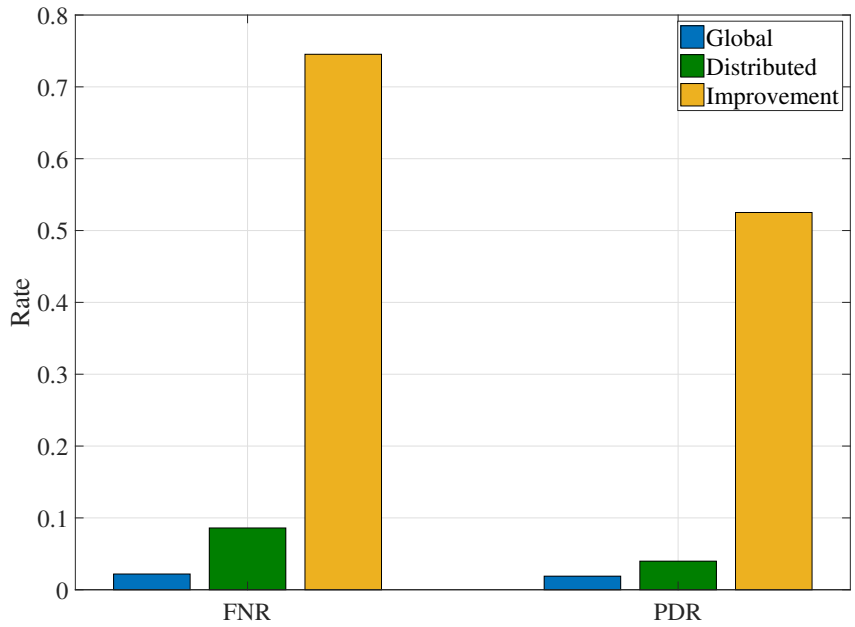


Figure 5.4: FNR and PDR in the network for global and distributed decision

lower in global decision. Therefore, the improvement in PDR in global decision is equal to 52%. As a conclusion, the global decision could improve the decision accuracy for the nodes that are located in-network coverage.

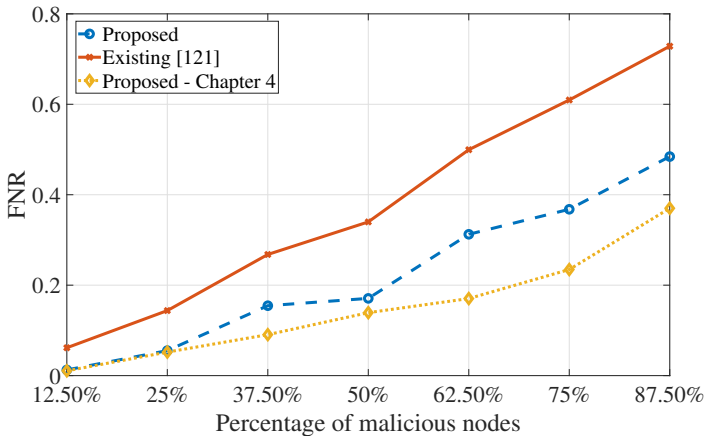
5.4 Performance Evaluation

The existing model in [121] is used to evaluate the performance of the proposed model. The impact of various rates of malicious nodes on the false alarm rate is studied on the proposed model and existing model.

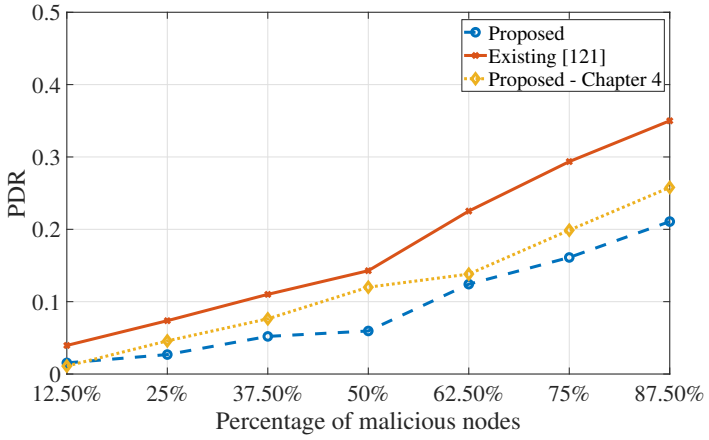
5.4.1 Effect of Selective Forwarding Attack on FNR

Generally, when the model has a low FNR, it is able to detect the most malicious nodes. The result that is shown in Figure 5.5 (a) represents the FNR for various percentages of malicious nodes. The following remarks can be made:

- in the existing model, the FNR reaches to 0.73 when the percentage of malicious nodes is



(a) FNR



(b) PDR

Figure 5.5: Effect of various percentage of selective forwarding attackers on: a)FNR; b)PDR

equal to 87.50%.

- FNR values in the proposed model is reduced. Thus, the global decision has the minimum FNR value for all rates of malicious nodes.

5.4.2 Effect of Selective Forwarding Attack on PDR

To measure the model performance, the PDR with different percentage of malicious nodes is studied as shown in Figure 5.5 (b). Generally, the PDR is increasing when the percentage of malicious nodes is increasing. In addition, the existing model produces high PDR which results from the high FNR. On the other hand, the proposed model has lower PDR which improves the network performance.

5.4.3 Measuring the Improvement Rate

The improvement rate on FNR and PDR for the proposed model in comparison with the existing model [121] is measured. As shown in Figure 5.6, the FNR is highly improved in the proposed model when the percentage of malicious nodes is equal to 12.50%. In addition, the rate at 50%, which is a high percentage, increases again to around 50%. As a result, the proposed model provides high improvement on PDR in comparison with the existing model, thus, it gains better network performance.

5.5 Summary

In this chapter, a global roaming trust-based model for the V2X network was proposed. Various malicious behavior were considered to study the performance of the proposed model, which are selective forwarding attack, bad-mouthing attack and good-mouthing attack. Various experiments with different percentage of malicious nodes were conducted. Comparison results showed that the proposed model improved FNR by 33.5% and PDR by 40% when the percentage of malicious nodes is equal to 87.50%. The main conclusions are:

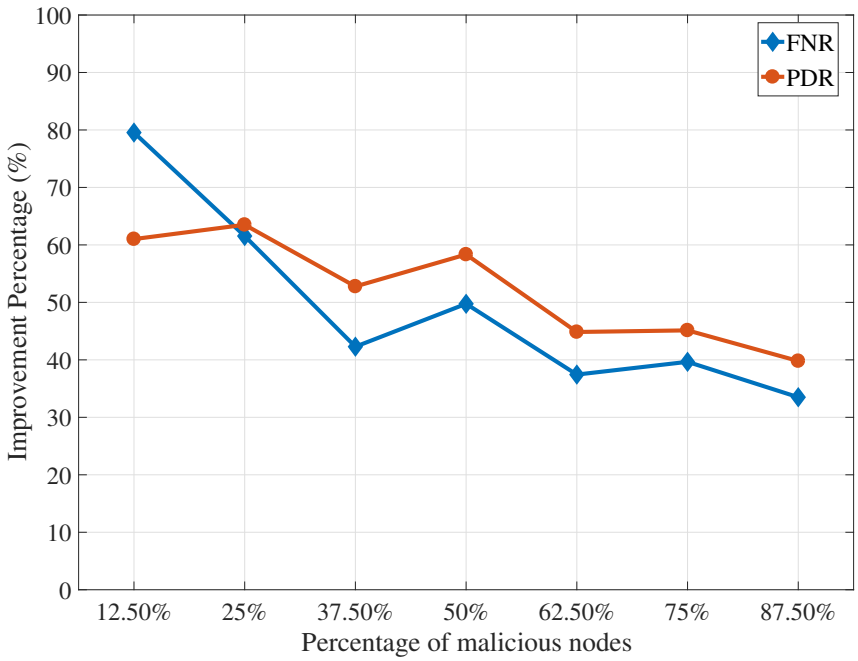


Figure 5.6: Improvement rate on FNR and PDR in the proposed model

- The local decision is considered as a support for the global decision. The combination of local and global blacklist gives very low values of FNR, FPR and PDR.
- The global decision system improved the trust decision where the road entity has a global knowledge regarding the other malicious nodes in the network. As a result, it minimizes the chance of communicating with malicious nodes.
- Various experiments were conducted to set-up the simulation parameters. The optimal value for each threshold was chosen based on the simulation results.
- In addition to malicious road entities, two RSU attacks were studied which are bad-mouthing and good-mouthing attacks. The high impact of good mouthing attack on FPR was noticed in comparison with a bad-mouthing attack where FNR was affected.
- The performance evaluation was made for the proposed model by comparing it with the

existing model. The results showed high improvement in FNR and PDR. Thus, it increases network performance by minimizing the number of dropped packets.

Chapter 6

Concluding Remarks

In this thesis, an in-depth analysis of V2X communications in three dimensions is conducted. The first dimension includes the ability of security services in IEEE802.11p and LTE-V2X to defend against various cyber-attacks. The second dimension covers the security challenges for various security solutions which ensure trusted communication in vehicular networks. The third dimension is about electing trusted communication links which provide QoS in V2X network. Building on the comprehensive review (in Chapter 2), a new algorithm is introduced for enhancing the QoS in V2X communications. The channel model for LTE-V2X (release 14) was investigated for the first time by studying the link outage probability in various scenarios. Based on the results, the proposed algorithm improved the link quality by choosing the most trusted link.

Moreover, a new trust model is designed for protecting V2X communication against internal attackers (in Chapter 4). The model is a recommendation-based where the neighboring nodes collaborate in the trust evaluation process. It has a novelty in collecting recommendations and the computing of indirect trust. Also, non-stable malicious behaviors were proposed in the adversary model for the first time in vehicular networks. Total trust value is evaluated based on various communication scenarios in a vehicular network. A theoretical analysis of the proposed

model was conducted to validate the simulation. To assess the performance, I have compared the proposed model with an existing recommendation-based trust model. The results showed that the proposed model outperforms the existing one.

In addition, the proposed model (in Chapter 4) was improved by expanding it to have a global decision system. The global roaming trust-based model was introduced (in Chapter 5). It gives the road entities the ability to has a global knowledge regarding malicious nodes in the network. Also, RSU attacks were proposed to evaluate the ability of the proposed model to protect the network against them.

6.1 Limitations

The main aim of this thesis was to design models that achieve trusted communications in V2X networks. However, there are certain limitations while exploring the aim of this thesis. It is expected that these points will help with further research:

- Due to the unexisting of V2X communications with LTE-A (release 14) in the real world, there is a lack of real communication data for V2X communications.
- The main focus of this thesis is on the trustworthiness in ad-hoc connections between road entities because of lack of time.
- Because of the limited scope of thesis on trusted communications regardless of the message content, the proposed models only considered link and node trustworthiness.

6.2 Future Work

In this final subsection, further interesting research topics related to the work proposed in this thesis are discussed. In future work, the proposed models could be tested using real communication data. Also, the proposed QoS-based algorithm (in Chapter 3) could be extended

to include the trusted cellular link. A new algorithm could be designed to choose the optimal route between D2D and cellular connections for delivering the packets to the core network. In addition, the message content could be evaluated by measuring the received data correctness. In addition, the current research could be improved in the following ways:

- The decision system in Chapter 5 could be developed to make more accurate decisions.
- Increase the number of road entities in Chapter 4 and Chapter 5 and check the difference in network performance.
- Study different metrics for evaluating the link in Chapter 3.
- Expand the study of current research in routing packets in vehicular network to be a complete survey.
- Implement a new decision system between the decision of distributed and global trust models.
- Apply the current models in a network simulator.
- Apply different multi-metric algorithms and study the performance and complexity for each one.

Bibliography

1. Araniti, G., Campolo, C., Condoluci, M., Iera, A. & Molinaro, A. LTE for vehicular networking: a survey. *IEEE Communications Magazine* **51,** 148–157 (2013) (*p.* 2).
2. Siemens. *Vehicle-to-X (V2X) communication technology* technical report (Siemens, 2015) (*p.* 2).
3. Ahmed, K. J. & Lee, M. J. Secure, LTE-based V2X Service. *IEEE Internet of Things Journal* **5,** 3724–3732 (2017) (*pp.* 2, 9).
4. Alnasser, A., Sun, H. & Jiang, J. Cyber security challenges and solutions for V2X communications: A survey. *Computer Networks* **151,** 52–67 (2019) (*pp.* 3, 85).
5. Hamida, E. B., Noura, H. & Znaidi, W. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics* **4,** 380–423 (2015) (*pp.* 7, 10, 48).
6. *Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancement for V2X services (3GPP TS 23.285 version 14.2.0 Release 14)* technical report (ETSI, 2017) (*pp.* 9, 11–12, 14, 16–17).
7. Schlienz J, R. A. *Whitepaper: Device to Device Communication in LTE* technical report (ROHDE & SCHWARZ, 2015) (*pp.* 9, 18).

8. Filippi, A., Moerman, K., Martinez, V., Semiconductors, A. T., Haran, O. & Toledano, R. *IEEE802.11p ahead of LTE-V2V for safety applications* technical report (NXP Semiconductors & Autotalks, 2017) (*p.* 12).

9. Dawood, M., Fuhrmann, W. & Ghita, B. V. *Assay of White Space Technology Standards for Vehicular Cognitive Access* in *Proc. of the 10th International Network Conference (INC)* (), 23–33 (*p.* 12).

10. IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages. *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013),* 1–240 (2016) (*pp.* 12, 19).

11. Laurendeau, C. & Barbeau, M. *Threats to Security in DSRC/WAVE* in *International Conference on Ad-Hoc Networks and Wireless* (2006), 266–279 (*pp.* 12, 21–23).

12. Asadi, A., Wang, Q. & Mancuso, V. A survey on device-to-device communication in cellular networks. *IEEE Communications Surveys & Tutorials* **16,** 1801–1819 (2014) (*pp.* 14–15).

13. Liu, J., Kato, N., Ma, J. & Kadowaki, N. Device-to-Device Communication in LTE-Advanced Networks: A Survey. *IEEE Communications Surveys Tutorials* **17,** 1923–1940. ISSN: 1553-877X (2015) (*p.* 15).

14. Zhang, M. & Fang, Y. Security analysis and enhancements of 3GPP authentication and key agreement protocol. *IEEE Transactions on wireless communications* **4,** 734–742 (2005) (*p.* 18).

15. 5G-Americas. *V2X Cellular Solutions* technical report (2016) (*p.* 18).

16. Hsu, R.-H. & Lee, J. *Group anonymous D2D communication with end-to-end security in LTE-A* in *IEEE Conference on Communications and Network Security (CNS)* (2015), 451–459 (*pp.* 18, 23).

17. Yan, Z., Xie, H., Zhang, P. & Gupta, B. B. Flexible data access control in D2D communications. *Future Generation Computer Systems* **82,** 738–751 (2017) (*p.* 18).

18. Kerrache, C. A., Calafate, C. T., Cano, J.-C., Lagraa, N. & Manzoni, P. Trust management for Vehicular Networks: An Adversary-Oriented Overview. *IEEE Access* **4,** 9293–9307 (2016) (*pp.* 19, 21, 24, 39).

19. Mokhtar, B. & Azab, M. Survey on security issues in vehicular ad hoc networks. *Alexandria Engineering Journal* **54,** 1115–1126 (2015) (*pp.* 20, 22–23).

20. Seddigh, N., Nandy, B., Makkar, R. & Beaumont, J.-F. *Security advances and challenges in 4G wireless networks* in *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on* (2010), 62–71 (*pp.* 20, 22–23).

21. Al-Kahtani, M. S. *Survey on security attacks in Vehicular Ad hoc Networks (VANETs)* in *the 6th International Conference on Signal Processing and Communication Systems (ICSPCS)* (2012), 1–9 (*pp.* 21, 29, 83).

22. Cheng, Y., Fu, X., Du, X., Luo, B. & Guizani, M. A lightweight live memory forensic approach based on hardware virtualization. *Information Sciences* **379,** 23–41 (2017) (*p.* 22).

23. Mejri, M. N., Ben-Othman, J. & Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications* **1,** 53–66 (2014) (*p.* 22).

24. Fonseca, E. & Festag, A. A survey of existing approaches for secure ad hoc routing and their applicability to VANETS. *NEC network laboratories* **28,** 1–28 (2006) (*p.* 24).

25. Ghafghazi, H., El Mougy, A. & Mouftah, H. T. *Enhancing the privacy of LTE-based public safety networks* in *the 39th IEEE Conference on Local Computer Networks Workshops (LCN Workshops)* (2014), 753–760 (*p.* 24).

26. Haus, M., Waqas, M., Ding, A. Y., Li, Y., Tarkoma, S. & Ott, J. Security and Privacy in Device-to-Device (D2D) Communication: A Review. *IEEE Communications Surveys & Tutorials* **19,** 1054–1079 (2017) (*p.* 26).

27. Du, X., Xiao, Y., Ci, S., Guizani, M. & Chen, H.-. *A Routing-Driven Key Management Scheme for Heterogeneous Sensor Networks* in *Proc. of the IEEE International Conference on Communications* (June 2007), 3407–3412 (*p.* 26).

28. Boneh, D., Di Crescenzo, G., Ostrovsky, R. & Persiano, G. *Public key encryption with keyword search* in *International Conference on the Theory and Applications of Cryptographic Techniques* (2004), 506–522 (*p.* 27).

29. Li, G., Ma, M., Liu, C. & Shu, Y. *A Lightweight Secure VANET-Based Navigation System* in *Proc. of the IEEE Conference on Global Communications (GLOBECOM)* (2015), 1–6 (*p.* 27).

30. Abdelgader, A. M. & Shu, F. *Exploiting the physical layer security for providing a simple user privacy security system for vehicular networks* in *International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE)* (2017), 1–6 (*p.* 27).

31. Bhoi, S. K. & Khilar, P. M. SIR: a secure and intelligent routing protocol for vehicular ad-hoc network. *IET Networks* **4,** 185–194 (2014) (*pp.* 27, 38, 41).

32. Shukla, N., Dinker, A. G., Srivastava, N. & Singh, A. *Security in vehicular ad hoc network by using multiple operating channels* in *the 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (2016), 3064–3068 (*pp.* 27, 38, 49).

33. Hong, X., Huang, D., Gerla, M. & Cao, Z. *SAT: Situation-Aware Trust architecture for vehicular networks* in *Proc. of the 3rd international workshop on Mobility in the evolving internet architecture* (2008), 31–36 (*p.* 28).

34. Zhang, L. OTIBAAGKA: A New Security Tool for Cryptographic Mix-Zone Establishment in Vehicular Ad Hoc Networks. *IEEE Transactions on Information Forensics and Security* **12,** 2998–3010 (2017) (*pp.* 28, 36, 41).

35. Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A. & Sun, Z. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Internet of Things Journal* **4,** 1832–1843 (2017) (*pp.* 28, 36).

36. Wan, J., Lopez, A. B. & Al Faruque, M. A. *Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security* in *Proc. of the 7th International Conference on Cyber-Physical Systems* (2016) (*p.* 28).

37. Zhu, X., Xu, F., Novak, E., Tan, C. C., Li, Q. & Chen, G. Using Wireless Link Dynamics to Extract a Secret Key in Vehicular Scenarios. *IEEE Transactions on Mobile Computing* **16,** 2065–2078 (2017) (*pp.* 29, 36).

38. Chuang, M.-C. & Lee, J.-F. TEAM: Trust-Extended Authentication Mechanism for vehicular ad hoc networks. *IEEE systems journal* **8,** 749–758 (2014) (*pp.* 29, 36, 38, 81).

39. Yang, Y., Wei, Z., Zhang, Y., Lu, H., Choo, K.-K. R. & Cai, H. V2X security: A case study of anonymous authentication. *Pervasive and Mobile Computing* **41,** 259–269 (2017) (*p.* 29).

40. Mamun, M. S. I., Miyaji, A. & Takada, H. *A multi-purpose group signature for vehicular network security* in *the 17th International Conference on Network-Based Information Systems (NBiS)* (2014), 511–516 (*p.* 29).

41. Ying, B. & Nayak, A. Anonymous and Lightweight Authentication for Secure Vehicular Networks. *IEEE Transactions on Vehicular Technology* **66,** 10626–10636 (2017) (*pp.* 29, 41).

42. Sun, C., Liu, J., Xu, X. & Ma, J. A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs. *IEEE Access* **5,** 24012–24022 (2017) (*pp.* 29, 36).

43. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K. & Khan, A. W. TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network. *IEEE Sensors Journal* **15,** 6962–6972 (2015) (*p.* 30).

44. Gazdar, T., Rachedi, A., Benslimane, A. & Belghith, A. *A distributed advanced analytical trust model for VANETs* in *Proc. of the IEEE conference on Global Communications (GLOBECOM)* (2012), 201–206 (*pp.* 30, 40).

45. Kerrache, C. A., Lagraa, N., Calafate, C. T., Cano, J.-C. & Manzoni, P. T-VNets: A novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS. *Computer Communications* **93,** 68–83 (2016) (*pp.* 30, 36, 42).

46. Patel, K. N. & Jhaveri, R. H. Isolating Packet Dropping Misbehavior in VANET using Ant Colony Optimization. *International Journal of Computer Applications* **120** (2015) (*p.* 30).

47. Wei, Z., Yu, F. R. & Boukerche, A. *Trust based security enhancements for vehicular ad–hoc networks* in *Proc. of the 4th ACM international symposium on Development and analysis of intelligent vehicular networks and applications* (2014), 103–109 (*pp.* 30, 41).

48. Abdelaziz, K. C., Lagraa, N. & Lakas, A. *Trust model with delayed verification for message relay in VANETs* in *International Wireless Communications and Mobile Computing Conference (IWCMC)* (2014), 700–705 (*p.* 30).

49. Golle, P., Greene, D. & Staddon, J. *Detecting and correcting malicious data in VANETs* in *Proc. of the 1st ACM international workshop on Vehicular ad hoc networks* (2004), 29–37 (*p.* 30).

50. Yang, N. A similarity based trust and reputation management framework for VANETs. *International Journal of Future Generation Communication and Networking* **6,** 25–34 (2013) (*p.* 31).

51. Ding, Q., Li, X., Jiang, M. & Zhou, X. *Reputation-based trust model in vehicular ad hoc networks* in *International Conference on Wireless Communications and Signal Processing (WCSP)* (2010), 1–6 (*p.* 31).

52. Dixit, K., Pathak, P. & Gupta, S. *A new technique for trust computation and routing in VANET* in *Symposium on Colossal Data Analysis and Networking (CDAN)* (2016), 1–6 (*pp.* 31, 42).

53. Rostamzadeh, K., Nicanfar, H., Torabi, N., Gopalakrishnan, S. & Leung, V. C. A context-aware trust-based information dissemination framework for vehicular networks. *IEEE Internet of Things Journal* **2,** 121–132 (2015) (*pp.* 31, 36, 40, 81).

54. Li, X., Liu, J., Li, X. & Sun, W. *RGTE: a Reputation-based Global Trust Establishment in VANETs* in *Proc. of the 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS)* (2013), 210–214 (*pp.* 31, 47).

55. Khan, U., Agrawal, S. & Silakari, S. Detection of malicious nodes (DMN) in vehicular ad-hoc networks. *Procedia Computer Science* **46,** 965–972 (2015) (*pp.* 31, 37, 40).

56. Shen, W., Liu, L., Cao, X., Hao, Y. & Cheng, Y. Cooperative message authentication in vehicular cyber-physical systems. *IEEE Transactions on Emerging Topics in Computing* **1,** 84–97 (2013) (*pp.* 32, 41, 81).

57. Haddadou, N., Rachedi, A. & Ghamri-Doudane, Y. *Trust and exclusion in vehicular ad hoc networks: an economic incentive model based approach* in *Proc. of Computing, Communications and IT Applications Conference (ComComAp)* (2013), 13–18 (*p.* 32).

58. Haddadou, N., Rachedi, A. & Ghamri-Doudane, Y. A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology* **64,** 3657–3674 (2015) (*pp.* 32, 36).

59. Jesudoss, A., Raja, S. K. & Sulaiman, A. Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme. *Ad Hoc Networks* **24,** 250–263 (2015) (*pp.* 32, 37).

60. Kerrache, C. A., Lagraa, N., Calafate, C. T. & Lakas, A. *TROUVE: A Trusted ROuting protocol for Urban Vehicular Environments* in *Proc. of the 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (2015), 260–267 (*p.* 32).

61. Zhang, Y., Wang, L. & Sun, W. Trust system design optimization in smart grid network infrastructure. *IEEE Transactions on Smart Grid* **4,** 184–195 (2013) (*pp.* 32, 94).

62. Mármol, F. G. & Pérez, G. M. TRIP, a Trust and Reputation Infrastructure-based Proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications* **35,** 934–941 (2012) (*pp.* 33, 40, 81).

63. Rafique, N., Khan, M. A., Saqib, N. A., Bashir, F., Beard, C. & Li, Z. BlackHole Prevention in VANETs Using Trust Management and Fuzzy Logic Analyzer. *International Journal of Computer Science and Information Security* **14,** 1226 (2016) (*pp.* 33, 42).

64. Ding, Q., Li, X., Jiang, M. & Zhou, X. *Reputation management in vehicular ad hoc networks* in *International Conference on Multimedia Technology (ICMT)* (2010), 1–5 (*p.* 33).

65. Fan, Q. G., Wang, L., Cai, Y. N., Li, Y. Q. & Chen, J. *VANET Routing Replay Attack Detection Research Based on SVM* in *Proc. of Conferences on MATEC Web* (2016) (*pp.* 33, 41).

66. Kim, M., Jang, I., Choo, S., Koo, J. & Pack, S. *Collaborative security attack detection in software-defined vehicular networks* in *the 19th Asia-Pacific conference on Network Operations and Management Symposium (APNOMS)* (2017), 19–24 (*pp.* 33, 41).

67. Sedjelmaci, H. & Senouci, S. M. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Computers & Electrical Engineering* **43,** 33–47 (2015) (*pp.* 33, 36–37, 42).

68. Li, W. & Song, H. ART: An Attack-Resistant Trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems* **17,** 960–969 (2016) (*p.* 33).

69. Huang, X., Yu, R., Kang, J. & Zhang, Y. Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks. *IEEE Access* **5,** 25408–25420 (2017) (*pp.* 34, 36).

70. Chen, C., Zhang, J., Cohen, R. & Ho, P.-H. *A trust modeling framework for message propagation and evaluation in VANETs* in *the 2nd International Conference on Information Technology Convergence and Services (ITCS)* (2010), 1–8 (*pp.* 34, 37).

71. Jahan, R. & Suman, P. *Detection of malicious node and development of routing strategy in VANET* in *Proc. of the 3rd International Conference on Signal Processing and Integrated Networks (SPIN)* (2016), 472–476 (*pp.* 34, 49).

72. Zhang, D., Yu, F. R., Wei, Z. & Boukerche, A. Trust-based Secure Routing in Software-defined Vehicular Ad-Hoc Networks. *arXiv journal* (2016) (*pp.* 34, 49).

73. Wu, L., Du, X. & Wu, J. Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms. *IEEE Transactions on Vehicular Technology* **65,** 6678–6691. ISSN: 0018-9545 (2016) (*p.* 34).

74. Shaikh, R. A. & Alzahrani, A. S. Intrusion-aware trust model for vehicular ad hoc networks. *Security and communication networks* **7,** 1652–1669 (2014) (*pp.* 34, 40–41).

75. Tajeddine, A., Kayssi, A. & Chehab, A. *A privacy-preserving trust model for VANETs* in *the 10th IEEE conference on Computer and Information Technology (CIT)* (2010), 832–837 (*pp.* 35, 41).

76. Chen, Y.-M. & Wei, Y.-C. A beacon-based trust management system for enhancing user centric location privacy in VANETs. *Journal of Communications and Networks* **15,** 153–163 (2013) (*pp.* 35, 40–41).

77. Raya, M. & Hubaux, J.-P. Securing vehicular ad hoc networks. *Journal of computer security* **15,** 39–68 (2007) (*p.* 35).

78. Kang, J., Yu, R., Huang, X., Jonsson, M., Bogucka, H., Gjessing, S. & Zhang, Y. Location privacy attacks and defenses in cloud-enabled internet of vehicles. *IEEE Wireless Communications* **23,** 52–59 (2016) (*pp.* 35, 40–41).

79. Sun, J., Zhang, C., Zhang, Y. & Fang, Y. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems* **21,** 1227–1239 (2010) (*pp.* 35–36, 41).

80. Al Mutaz, M., Malott, L. & Chellappan, S. *Leveraging platoon dispersion for sybil detection in vehicular networks* in *Proc. of the 11th Annual International Conference on Privacy, Security and Trust (PST)* (2013), 340–347 (*p.* 35).

81. Li, Q., Malip, A., Martin, K. M., Ng, S.-L. & Zhang, J. A reputation-based announcement scheme for VANETs. *IEEE Transactions on Vehicular Technology* **61,** 4095–4108 (2012) (*pp.* 36, 41).

82. Eiza, M. H., Owens, T. & Ni, Q. Secure and robust multi-constrained QoS aware routing algorithm for VANETs. *IEEE Transactions on Dependable and Secure Computing* **13,** 32–45 (2016) (*pp.* 36, 39, 43).

83. Harsch, C., Festag, A. & Papadimitratos, P. *Secure position-based routing for VANETs* in *the 66th IEEE Conference on Vehicular Technology* (2007), 26–30 (*pp.* 36, 39).

84. Harding, J., Powell, G., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J. & Wang, J. *Vehicle-to-vehicle communications: Readiness of V2V technology for application* technical report (National Highway Traffic Safety Administration, 2014) (*pp.* 38, 40).

85. Bali, R. S. & Kumar, N. Secure clustering for efficient data dissemination in vehicular cyber–physical systems. *Future Generation Computer Systems* **56,** 476–492 (2016) (*p.* 39).

86. Yan, G., Wen, D., Olariu, S. & Weigle, M. C. Security challenges in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems* **14,** 284–294 (2013) (*p.* 39).

87. Wei, Y.-c., Chen, Y.-m. & Shan, H.-l. *Beacon-based trust management for location privacy enhancement VANETs* in *Network Operations and Management Symposium (APNOMS)* (2011), 1–8 (*p.* 40).

88. El Zouka, H. A. *A Secure Interactive Architecture for Vehicular Cloud Environment* in *Proc. of IEEE International Conference on Smart Cloud (SmartCloud)* (2016), 254–261 (*p.* 41).

89. Eiza, M. H. & Ni, Q. An evolving graph-based reliable routing scheme for VANETs. *IEEE transactions on vehicular technology* **62,** 1493–1504 (2013) (*pp.* 42, 46, 52).

90. Li, G., Boukhatem, L. & Wu, J. Adaptive quality-of-service-based routing for vehicular ad hoc networks with ant colony optimization. *IEEE Transactions on Vehicular Technology* **66,** 3249–3264 (2017) (*pp.* 42, 52).

91. Korichi, A., Lakas, A. & Fekair, M. E. A. *An efficient QoS-compliant routing scheme for VANET* in *the 5th International conference on electronic devices, systems and applications (ICEDSA)* (2016), 1–4 (*pp.* 42, 52, 55).

92. Sun, Y., Luo, S., Dai, Q. & Ji, Y. An adaptive routing protocol based on QoS and vehicular density in urban VANETs. *International Journal of Distributed Sensor Networks* **11** (2015) (*pp.* 42, 52).

93. Liu, L., Chen, C., Wang, B., Zhou, Y. & Pei, Q. An Efficient and Reliable QoF Routing for Urban VANETs With Backbone Nodes. *IEEE Access* **7,** 38273–38286. ISSN: 2169-3536 (2019) (*pp.* 42, 46, 52).

94. Alzamzami, O. & Mahgoub, I. Fuzzy Logic-Based Geographic Routing for Urban Vehicular Networks Using Link Quality and Achievable Throughput Estimations. *IEEE Transactions on Intelligent Transportation Systems* **20,** 1–12. ISSN: 1524-9050 (2018) (*p.* 43).

95. Toutouh, J., Garcıéa-Nieto, J. & Alba, E. Intelligent OLSR routing protocol optimization for VANETs. *IEEE transactions on vehicular technology* **61,** 1884–1894 (2012) (*p.* 43).

96. Bitam, S. & Mellouk, A. *QoS swarm bee routing protocol for vehicular ad hoc networks* in *the IEEE International Conference on Communications (ICC)* (2011), 1–5 (*p.* 43).

97. Fekair, M. E. A., Lakas, A. & Korichi, A. *CBQoS-Vanet: Cluster-based artificial bee colony algorithm for QoS routing protocol in VANET* in *International conference on selected topics in mobile & wireless networking (MoWNeT)* (2016), 1–8 (*pp.* 43, 46).

98. Eiza, M. H., Owens, T., Ni, Q. & Shi, Q. Situation-aware QoS routing algorithm for vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology* **64,** 5520–5535 (2015) (*p.* 43).

99. Moridi, E. & Barati, H. RMRPTS: a Reliable Multi-level Routing Protocol with Tabu Search in VANET. *Telecommunication Systems* **65,** 127–137 (2017) (*p.* 43).

100. Zhang, G., Wu, M., Duan, W. & Huang, X. Genetic Algorithm Based QoS Perception Routing Protocol for VANETs. *Wireless Communications and Mobile Computing* **2018** (2018) (*p.* 43).

101. Chekkouri, A. S., Ezzouhairi, A. & Pierre, S. A new integrated VANET-LTE-A architecture for enhanced mobility in small cells HetNet using dynamic gateway and traffic forwarding. **140,** 15–27. ISSN: 1389-1286 (2018) (*pp.* 44, 46).

102. Wu, C., Yoshinaga, T., Chen, X., Zhang, L. & Ji, Y. Cluster-Based Content Distribution Integrating LTE and IEEE 802.11p with Fuzzy Logic and Q-Learning. *IEEE Computational Intelligence Magazine* **13,** 41–50. ISSN: 1556-603X (2018) (*pp.* 44, 53, 67–68, 76).

103. E. m. Zhioua, G., Tabbane, N., Labiod, H. & Tabbane, S. A Fuzzy Multi-Metric QoS-Balancing Gateway Selection Algorithm in a Clustered VANET to LTE Advanced Hybrid Cellular Network. *IEEE Transactions on Vehicular Technology* **64,** 804–817. ISSN: 0018-9545 (2015) (*pp.* 44, 46).

104. Ucar, S., Ergen, S. C. & Ozkasap, O. Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination. *IEEE Transactions on Vehicular Technology* **65,** 2621–2636. ISSN: 0018-9545 (2016) (*pp.* 44, 46).

105. Mir, Z. H., Kim, J., Ko, Y.-B. & Filali, F. *Improved Multi-hop Routing in Integrated VANET-LTE Hybrid Vehicular Networks* in *Proc. of the 10th ACM International Conference on Ubiquitous Information Management and Communication* (2016), 76:1–76:6 (*pp.* 44, 46).

106. Liu, J., Kawamoto, Y., Nishiyama, H., Kato, N. & Kadowaki, N. Device-to-device communications achieve efficient load balancing in LTE-advanced networks. *IEEE Wireless Communications* **21,** 57–65. ISSN: 1536-1284 (Apr. 2014) (*pp.* 44, 46, 53).

107. Liu, J., Zhang, S., Kato, N., Ujikawa, H. & Suzuki, K. Device-to-device communications for enhancing quality of experience in software defined multi-tier LTE-A networks. *IEEE Network* **29,** 46–52. ISSN: 0890-8044 (July 2015) (*pp.* 45, 53).

108. Tata, C. & Kadoch, M. *Multipath routing algorithm for device-to-device communications for public safety over LTE Heterogeneous Networks* in *Proc. of the 1st International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)* (2014), 1–7 (*pp.* 45–46, 53, 55).

109. Bastos, A. V., Silva, C. M. & da Silva, D. C. *Assisted routing algorithm for D2D communication in 5G wireless networks* in *Proc. of Wireless Days (WD) conference* (2018), 28–30 (*pp.* 45, 53).

110. Yang, M. J., Lim, S. Y., Park, H. J. & Park, N. H. Solving the data overload: Device-to-device bearer control architecture for cellular data offloading. *IEEE Vehicular Technology Magazine* **8,** 31–39 (2013) (*p.* 45).

111. Munir, D., Gu, J., Hasan, S. F. & Chung, M. Y. Reliable cooperative scheme for public safety services in LTE-A networks. *Transactions on emerging telecommunications technologies* **28,** e3008 (2017) (*pp.* 45–46).

112. Chi, K., Huang, L., Li, Y., Zhu, Y.-h., Tian, X.-z. & Xia, M. Efficient and reliable multicast using device-to-device communication and network coding for a 5G network. *IEEE Network* **31,** 78–84 (2017) (*pp.* 45, 53).

113. Liyanage, M., Kumar, P., Soderi, S., Ylianttila, M. & Gurtov, A. *Performance and security evaluation of intra-vehicular communication architecture* in *IEEE International Conference on Communications Workshops (ICC)* (2016), 302–308 (*p.* 47).

114. Hao, Y., Cheng, Y. & Ren, K. *Distributed key management with protection against RSU compromise in group signature based VANETs* in *IEEE Conference on Global Telecommunications (GLOBECOM)* (2008), 1–5 (*p.* 48).

115. Wang, J., Huang, Y., Feng, Z., Jiang, C., Zhang, H. & Leung, V. C. Reliable Traffic Density Estimation in Vehicular Network. *IEEE Transactions on Vehicular Technology* **67,** 6424–6437 (2018) (*p.* 48).

116. Zheng, Q., Zheng, K., Zhang, H. & Leung, V. C. Delay-optimal virtualized radio resource scheduling in software-defined vehicular networks via stochastic learning. *IEEE Transactions on Vehicular Technology* **65,** 7857–7867 (2016) (*p.* 49).

117. Zhang, Y., Zhang, H., Long, K., Zheng, Q. & Xie, X. Software-Defined and Fog-Computing-Based Next Generation Vehicular Networks. *IEEE Communications Magazine* **56,** 34–41 (2018) (*p.* 49).

118. *Study on channel model for frequencies from 0.5 to 100 GHz (3GPP TR 38.901 version 14.3.0 Release 14)* technical report (3GPP, 2018) (*p.* 54).

119. Karedal, J., Czink, N., Paier, A., Tufvesson, F. & Molisch, A. F. Path loss modeling for vehicle-to-vehicle communications. *IEEE transactions on vehicular technology* **60,** 323–328 (2010) (*pp.* 54, 56).

120. Socaciu, L., Giurgiu, O., Banyai, D. & Simion, M. PCM selection using AHP method to maintain thermal comfort of the vehicle occupants. *Energy Procedia* **85,** 489–497 (2016) (*pp.* 54, 58–60).

121. Shabut, A. M., Dahal, K. P., Bista, S. K. & Awan, I. U. Recommendation based trust model with an effective defence scheme for MANETs. *IEEE Transactions on Mobile Computing* **14,** 2101–2115 (2015) (*pp.* 82, 101, 110, 113, 137, 139).

122. Hu, H., Lu, R., Zhang, Z. & Shao, J. REPLACE: A reliable trust-based platoon service recommendation scheme in VANET. *IEEE Transactions on Vehicular Technology* **66,** 1786–1797 (2017) (*p.* 82).

123. Zhou, A., Li, J., Sun, Q., Fan, C., Lei, T. & Yang, F. A security authentication method based on trust evaluation in VANETs. *EURASIP Journal on Wireless Communications and Networking* **2015,** 59 (2015) (*p.* 82).

124. Ahmed, S. & Tepe, K. *Recommendation Trust for Improved Malicious Node Detection in Ad hoc Networks* in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)* (IEEE, 2017) (*p.* 82).

125. Zhang, J. *A survey on trust management for VANETs* in *IEEE conference on Advanced information networking and applications (AINA)* (2011), 105–112 (*p.* 83).

126. Alnasser, A. & Sun, H. A Fuzzy Logic Trust Model for Secure Routing in Smart Grid Networks. *IEEE Access* **5,** 17896–17903. ISSN: 2169-3536 (2017) (*pp.* 84, 95).

127. Alnasser, A. & Sun, H. *Performance analysis of behavior-based solutions in vehicular networks* in *Proc. of IEEE Conference on Computer Communications Workshops (INFOCOM)* (2018), 736–741 (*pp.* 85, 94).